

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ENRUTAMIENTO EN SOLUCIONES DE RED

Trabajo Colaborativo 4

Presenta

Alexander Belalcázar Gómez CC N° 94534321

Raúl Andrés Portela CC N° 94231532

Hermes Fernando Martínez CC N° 94302313

Enver Ricardo Pizo CC N° 94517159

Jose Luis Bedoya CC N° 94532863

Grupo: 34

Tutor

José Ignacio Cardona

Santiago de Cali, 18 de Mayo de 2017

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

Tabla de contenido

Introduccion

Objetivos

Laboratorio 4.4.1.2 Packet Tracer - Configure IP ACLs to Mitigate Attacks

Laboratorio 7.3.2.4 Packet Tracer - configuración básica de RIPv2 y RIPv6

Laboratorio 8.2.4.5 lab - configuring basic single-area ospfv2

Laboratorio 8.3.3.6 lab - configuring basic single-area ospfv3

Laboratorio 9.2.1.10 Packet Tracer - Configuring Standard ACLs

Laboratorio 9.2.1.11 Packet Tracer - Configuring Named Standard ACLs

Laboratorio 9.2.3.3 Packet Tracer - Configuring an ACL on VTY Lines

Laboratorio 9.5.2.6 Packet Tracer - Configuring IPv6 ACLs

Laboratorio 10.1.2.4 configuración de DHCPv4 básico en un router

Laboratorio 10.1.2.5 configuración de DHCPv4 básico en un switch

Laboratorio 10.2.3.5 configuración de dhcpv6 sin estado y con estado

Laboratorio 10.3.1.1 Packet Tracer - IdT y DHCP

Laboratorio 11.2.2.6 configuración de NAT dinámica y estática

Laboratorio 11.2.3.7 Configuración de un conjunto de nat con sobrecarga y pat

Conclusiones

Referencias

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



INTRODUCCION

En las telecomunicaciones, la manera como se crean y configuran las redes es muy importante para que la información y los datos funcionen correctamente. Consiste en una infraestructura física por medio de la cual se transporta la información desde la fuente hasta el destino, y con base en esa infraestructura se ofrecen a los usuarios los diversos servicios de telecomunicaciones. Con el siguiente trabajo se aprenderá a reconocer los conceptos de Enrutamiento dinámico, OSPF de una sola área, Listas de control de acceso, DHCP y traducción de direcciones IP para IPv4.

Las redes en general, consisten en "compartir recursos", y uno de sus objetivos es hacer que todos los programas, datos y equipo estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario. En otras palabras, el hecho de que el usuario se encuentre a 1000 km de distancia de los datos, no debe evitar que este los pueda utilizar como si fueran originados localmente.

Objetivo general: Reconocer los conceptos propios de enrutamiento los cuales involucran configuración de equipos que nos permita generar redes independientes sobre una misma infraestructura física.

Los objetivos trazados para este trabajo colaborativo son, obtener un aprendizaje basado en la práctica de los temas mencionados a continuación por medio del software packet tracer:

- Enrutamiento Dinámico.
- OSPF de una sola área
- Listas de control de acceso
- DHCP
- Traducción de direcciones IP para IPv4

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Desarrollo de la actividad

LABORATORIO 4.4.1.2 PACKET TRACER - CONFIGURE IP ACLS TO MITIGATE ATTACKS

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	Fa0/1	192.168.1.1	255.255.255.0	N/A	S1 Fa0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
	Lo0	192.168.2.1	255.255.255.0	N/A	N/A
R3	Fa0/1	192.168.3.1	255.255.255.0	N/A	S3 Fa0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 Fa0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 Fa0/18

Objectives

- ☐ Verify connectivity among devices before firewall configuration.
- ☐ Use ACLs to ensure remote access to the routers is available only from management station PC-C.
- ☐ Configure ACLs on R1 and R3 to mitigate attacks.
- ☐ Verify ACL functionality.

Background / Scenario

Access to routers R1, R2, and R3 should only be permitted from PC-C, the

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



management station. PC-C is also used for connectivity testing to PC-A, a server providing DNS, SMTP, FTP, and HTTPS services.

Standard operating procedure is to apply ACLs on edge routers to mitigate common threats based on source and/or destination IP address. In this activity, you create ACLs on edge routers R1 and R3 to achieve this goal. You then verify ACL functionality from internal and external hosts.

The routers have been pre-configured with the following:

- o Enable password: **ciscoenpa55**
- o Password for console: **ciscoconpa55**
- o Username for VTY lines: **SSHadmin**
- o Password for VTY lines: **ciscosshpa55**
- o IP addressing
- o Static routing

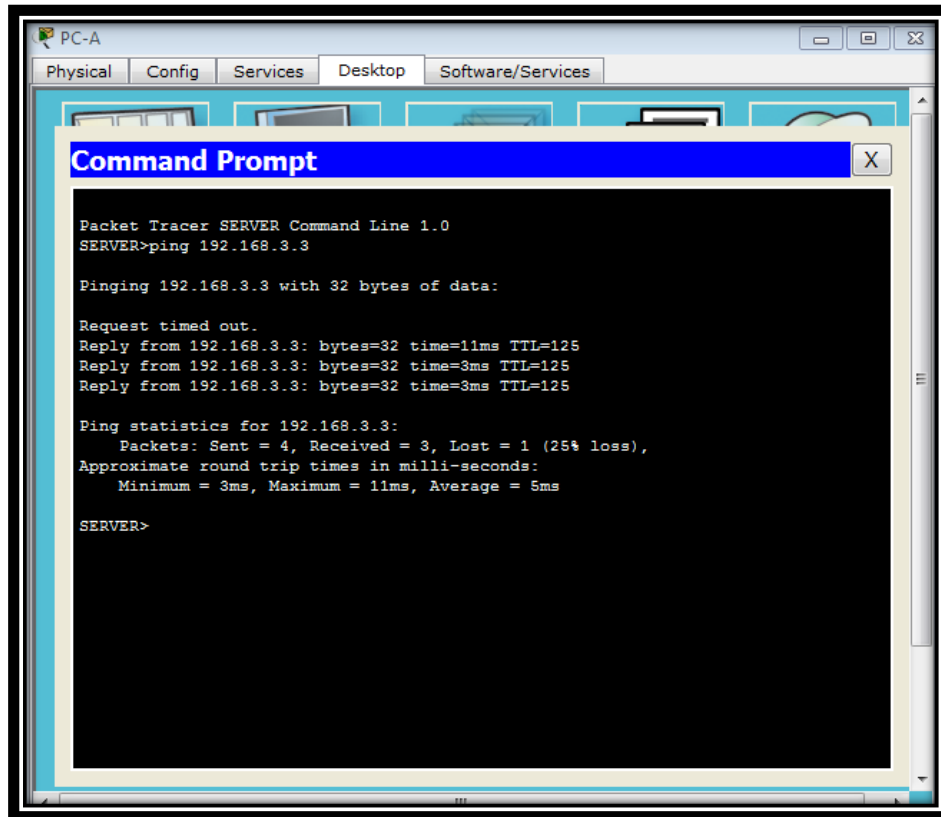
Part 1: Verify Basic Network Connectivity

Verify network connectivity prior to configuring the IP ACLs.

Step 1: From PC-A, verify connectivity to PC-C and R2.

- a. From the command prompt, ping **PC-C** (192.168.3.3).

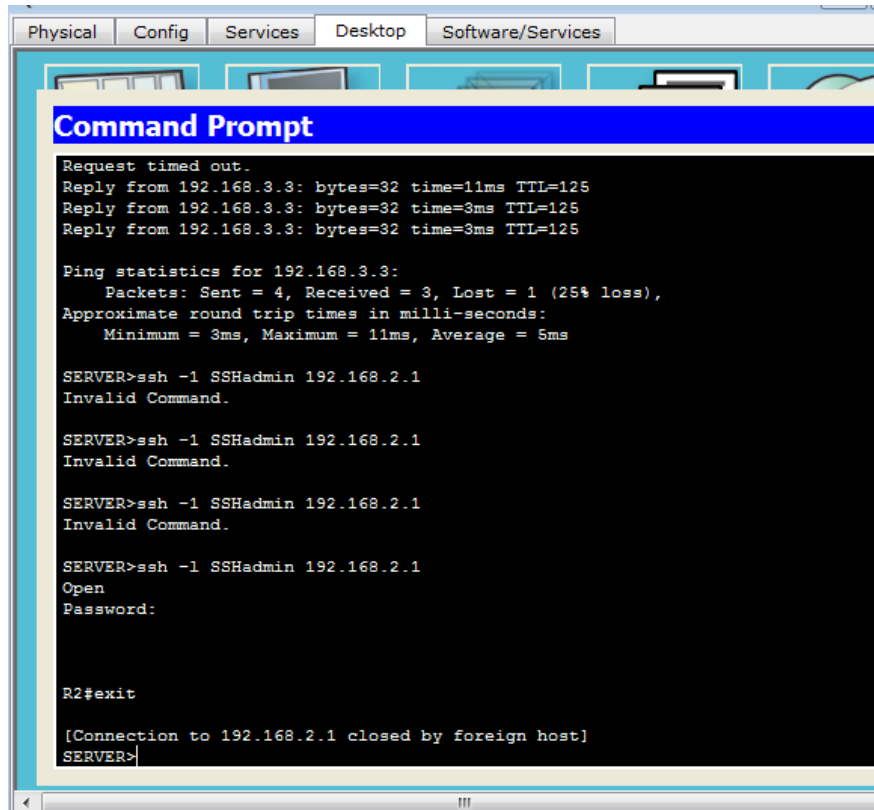
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



- b. From the command prompt, establish a SSH session to **R2** Lo0 interface (192.168.2.1) using username **SSHadmin** and password **ciscosshpa55**. When finished, exit the SSH session.

PC> **ssh -l SSHadmin 192.168.2.1**

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```

Physical Config Services Desktop Software/Services
Command Prompt
Request timed out.
Reply from 192.168.3.3: bytes=32 time=11ms TTL=125
Reply from 192.168.3.3: bytes=32 time=3ms TTL=125
Reply from 192.168.3.3: bytes=32 time=3ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 11ms, Average = 5ms

SERVER>ssh -l SSHAdmin 192.168.2.1
Invalid Command.

SERVER>ssh -l SSHAdmin 192.168.2.1
Invalid Command.

SERVER>ssh -l SSHAdmin 192.168.2.1
Invalid Command.

SERVER>ssh -l SSHAdmin 192.168.2.1
Open
Password:

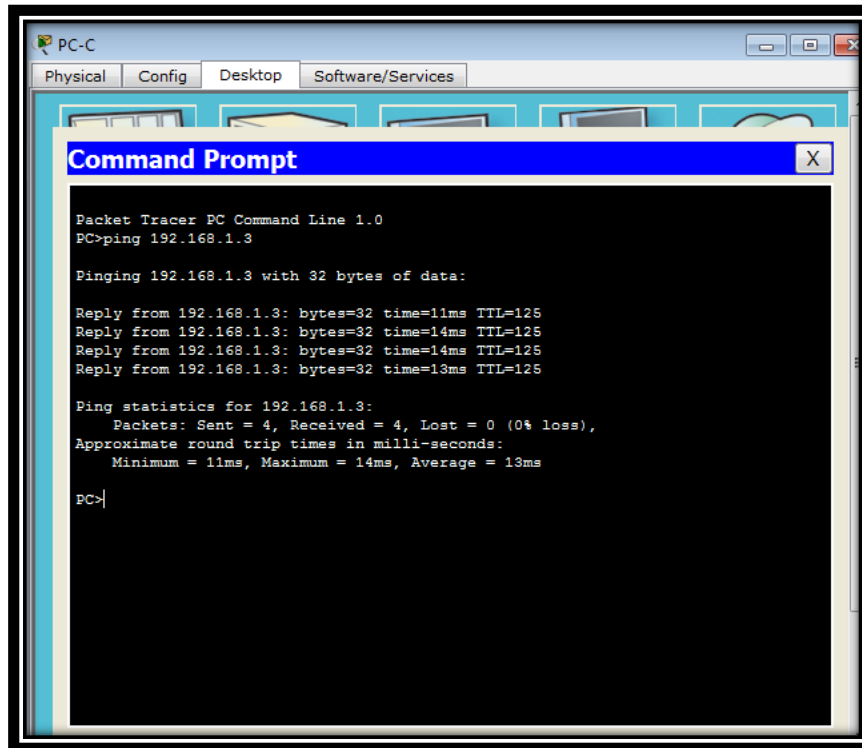
R2#exit

[Connection to 192.168.2.1 closed by foreign host]
SERVER>
  
```

Step 2: From PC-C, verify connectivity to PC-A and R2.

- a. From the command prompt, ping **PC-A** (192.168.1.3).

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```

PC-C
Physical Config Desktop Software/Services

Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

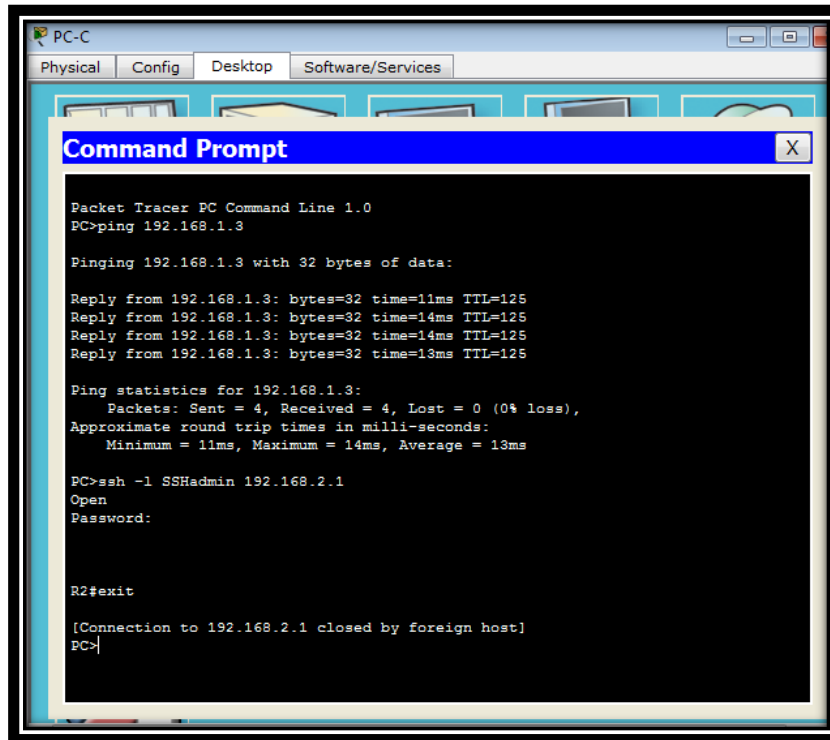
Reply from 192.168.1.3: bytes=32 time=11ms TTL=125
Reply from 192.168.1.3: bytes=32 time=14ms TTL=125
Reply from 192.168.1.3: bytes=32 time=14ms TTL=125
Reply from 192.168.1.3: bytes=32 time=13ms TTL=125

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 14ms, Average = 13ms

PC>
  
```

- b. From the command prompt, establish a SSH session to **R2** Lo0 interface (192.168.2.1) using username **SSHadmin** and password **ciscosshpa55**. Close the SSH session when finished.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```

PC-C
Physical Config Desktop Software/Services

Command Prompt

Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=11ms TTL=125
Reply from 192.168.1.3: bytes=32 time=14ms TTL=125
Reply from 192.168.1.3: bytes=32 time=14ms TTL=125
Reply from 192.168.1.3: bytes=32 time=13ms TTL=125

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 14ms, Average = 13ms

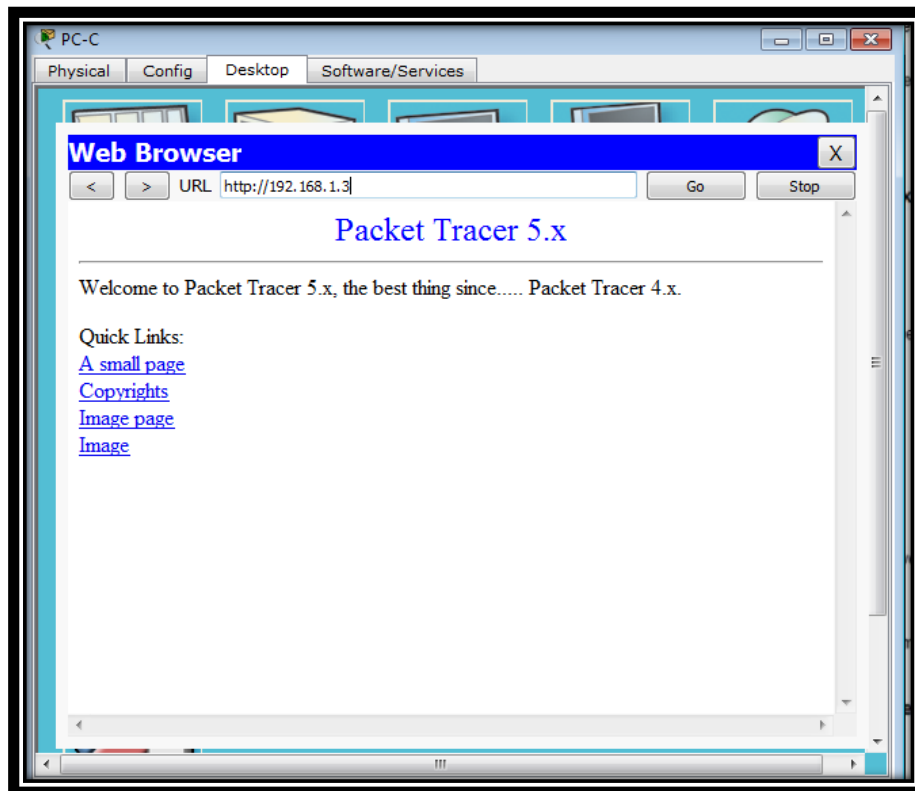
PC>ssh -l SSHadmin 192.168.2.1
Open
Password:

R2#exit

[Connection to 192.168.2.1 closed by foreign host]
PC>
  
```

- c. Open a web browser to the **PC-A** server (192.168.1.3) to display the web page.
Close the browser when done.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

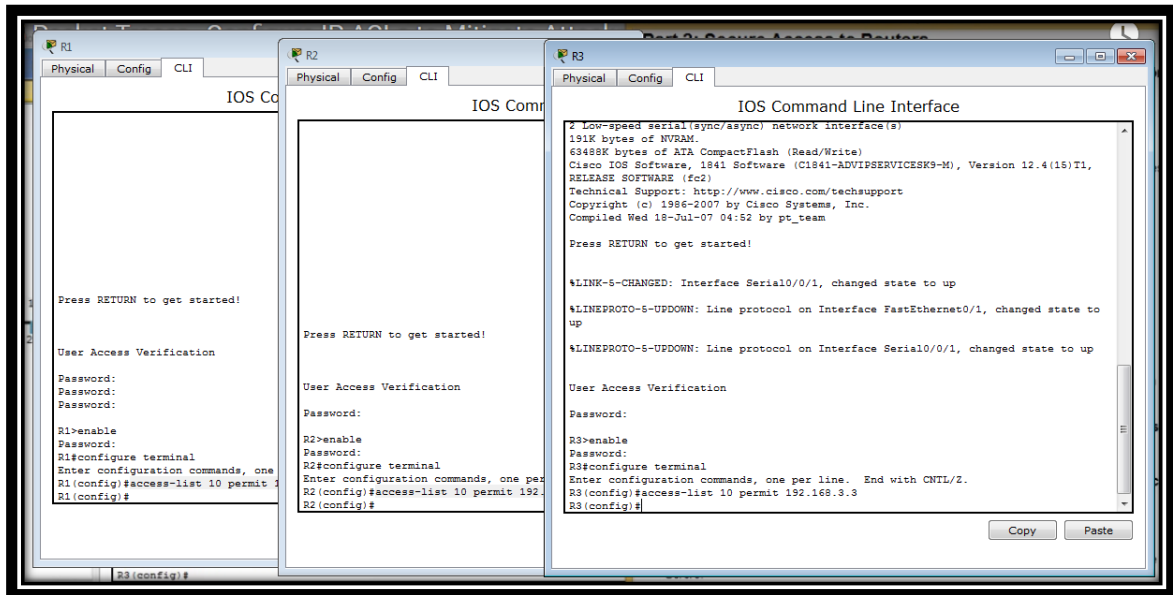


Part 2: Secure Access to Routers

Step 1: Configure ACL 10 to block all remote access to the routers except from PC-C.

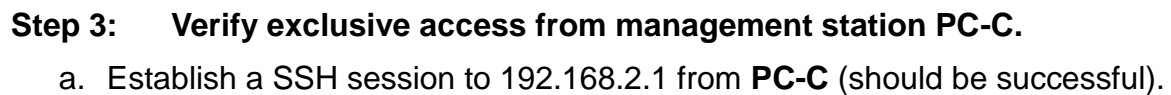
Use the **access-list** command to create a numbered IP ACL on **R1**, **R2**, and **R3**.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

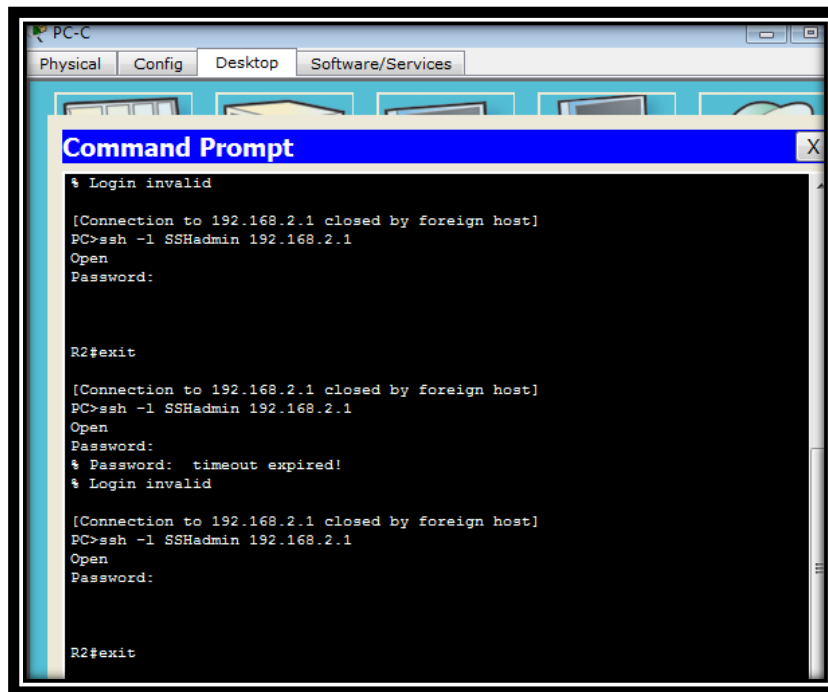


Step 2: Apply ACL 10 to ingress traffic on the VTY lines.

Use the **access-class** command to apply the access list to incoming traffic on the VTY lines.



UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
PC-C
Physical Config Desktop Software/Services

Command Prompt

% Login invalid

[Connection to 192.168.2.1 closed by foreign host]
PC>ssh -l SSHAdmin 192.168.2.1
Open
Password:

R2#exit

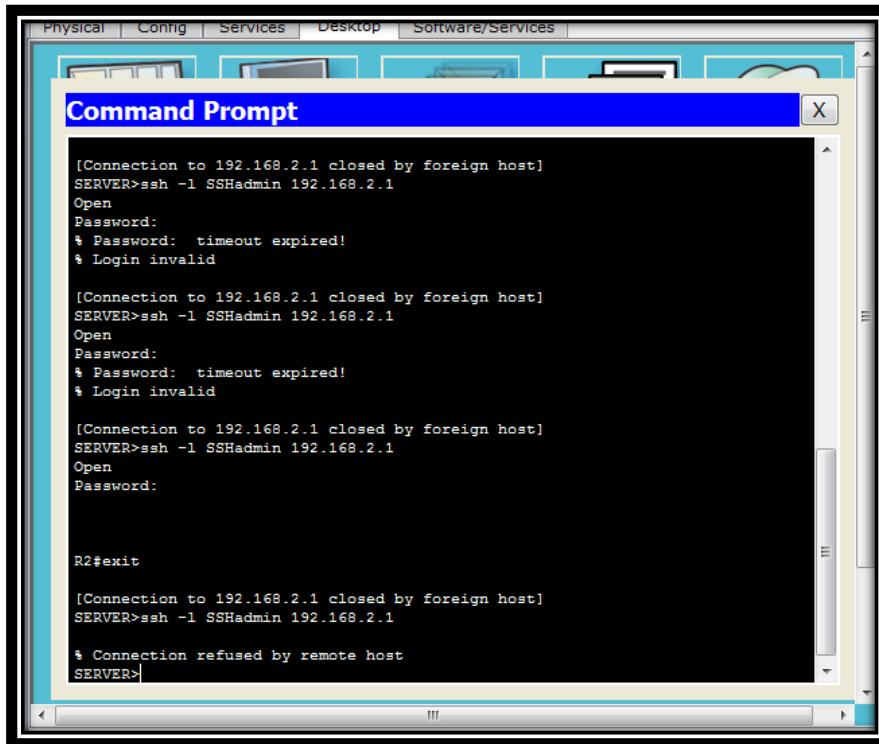
[Connection to 192.168.2.1 closed by foreign host]
PC>ssh -l SSHAdmin 192.168.2.1
Open
Password:
% Password: timeout expired!
% Login invalid

[Connection to 192.168.2.1 closed by foreign host]
PC>ssh -l SSHAdmin 192.168.2.1
Open
Password:

R2#exit
```

- b. Establish a SSH session to 192.168.2.1 from **PC-A** (should fail).

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
Physical  Config  Services  Desktop  Software/Services

Command Prompt

[Connection to 192.168.2.1 closed by foreign host]
SERVER>ssh -l SSHadmin 192.168.2.1
Open
Password:
% Password: timeout expired!
% Login invalid

[Connection to 192.168.2.1 closed by foreign host]
SERVER>ssh -l SSHadmin 192.168.2.1
Open
Password:
% Password: timeout expired!
% Login invalid

[Connection to 192.168.2.1 closed by foreign host]
SERVER>ssh -l SSHadmin 192.168.2.1
Open
Password:

R2#exit

[Connection to 192.168.2.1 closed by foreign host]
SERVER>ssh -l SSHadmin 192.168.2.1
% Connection refused by remote host
SERVER>
```

Part 3: Create a Numbered IP ACL 120 on R1

Permit any outside host to access DNS, SMTP, and FTP services on server **PC-A**, deny any outside host access to HTTPS services on **PC-A**, and permit **PC-C** to access **R1** via SSH.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

```
R1(config)#
R1(config)#
R1(config)#line vty 0 4
R1(config-line)#access-class 10 in
R1(config-line)#
R1(config-line)#exit
R1(config)#access-list 120 udp any host 192.168.1.3 eq domain
^
% Invalid input detected at '^' marker.

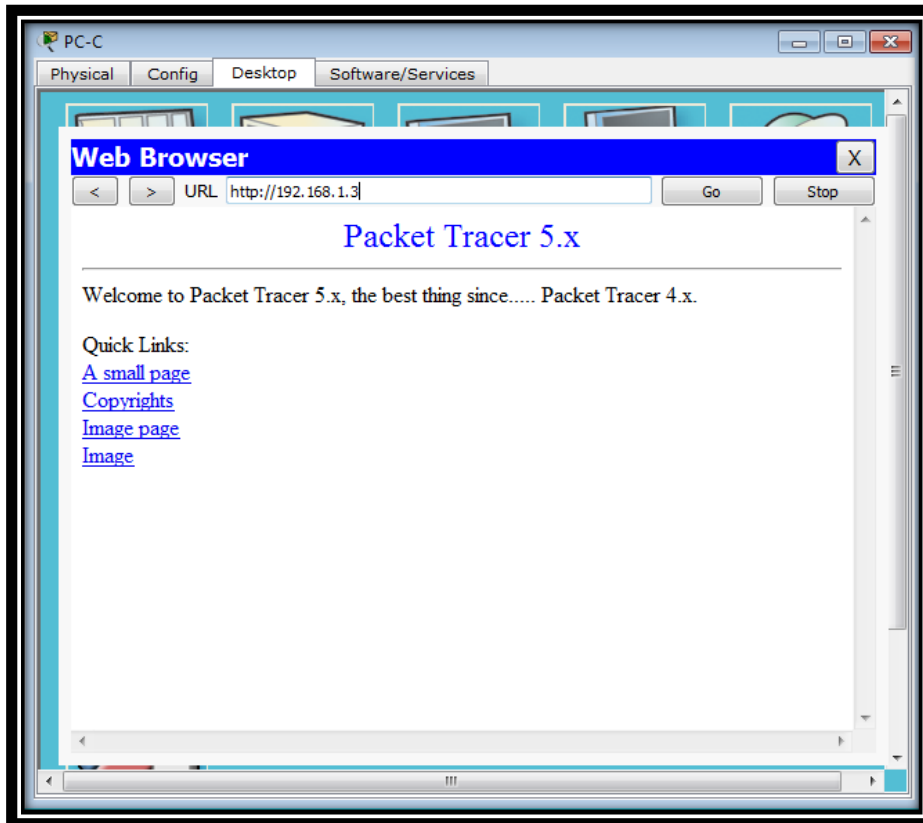
R1(config)#access-list 120 permit udp any host 192.168.1.3 eq domain
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq smtp
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq ftp
R1(config)#access-list 120 deny tcp any host 192.168.1 eq 443
^
% Invalid input detected at '^' marker.

R1(config)#access-list 120 deny tcp any host 192.168.1.3 eq 443
R1(config)#access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22
R1(config)#
```

Step 1: Verify that PC-C can access the PC-A via HTTPS using the web browser.

Be sure to disable HTTP and enable HTTPS on server **PC-A**.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Step 2: Configure ACL 120 to specifically permit and deny the specified traffic.

Use the **access-list** command to create a numbered IP ACL.

Step 3: Apply the ACL to interface S0/0/0.

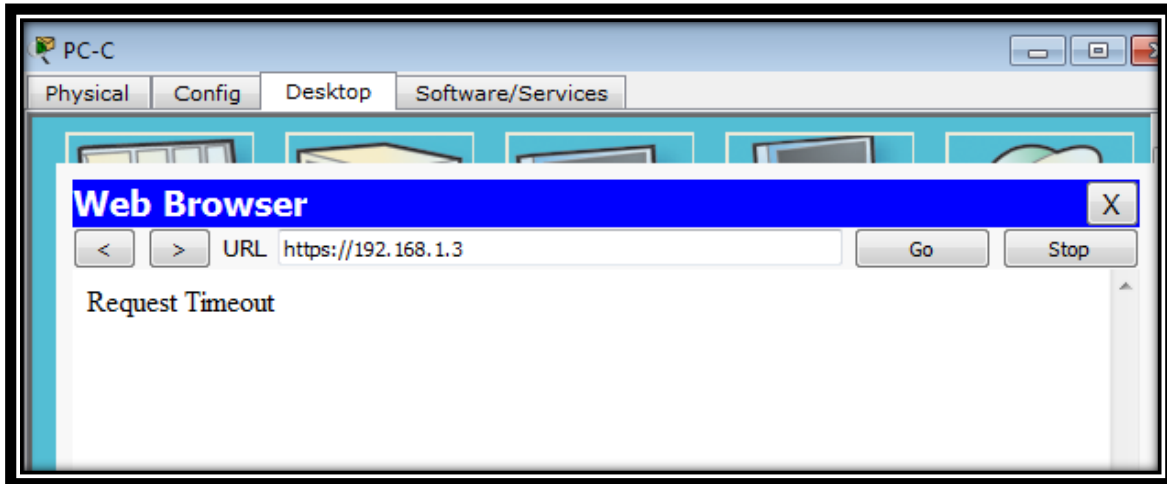
Use the **ip access-group** command to apply the access list to incoming traffic on interface S0/0/0.

```
R1(config)#interface s0/0/0
R1(config-if)#ip access-group 120 in
R1(config-if)#
```


UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Step 4: Verify that PC-C cannot access PC-A via HTTPS using the web browser.



Part 4: Modify An Existing ACL on R1

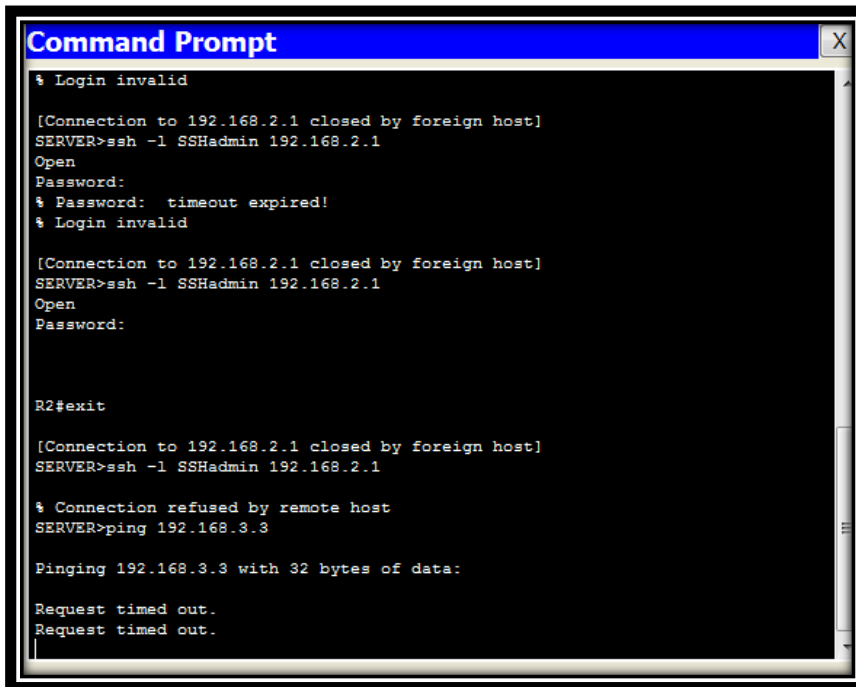
Permit ICMP echo replies and destination unreachable messages from the outside network (relative to **R1**); deny all other incoming ICMP packets.

```
R1(config)#access-list 120 permit icmp any any echo-reply
R1(config)#access-list 120 permit icmp any any unreachable
R1(config)#access-list 120 deny icmp any any
R1(config)#access-list 120 permit ip any any
R1(config)#
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Step 1: Verify that PC-A cannot successfully ping the loopback interface on R2.



```
Command Prompt
% Login invalid

[Connection to 192.168.2.1 closed by foreign host]
SERVER>ssh -l SSHadmin 192.168.2.1
Open
Password:
% Password: timeout expired!
% Login invalid

[Connection to 192.168.2.1 closed by foreign host]
SERVER>ssh -l SSHadmin 192.168.2.1
Open
Password:

R2#exit

[Connection to 192.168.2.1 closed by foreign host]
SERVER>ssh -l SSHadmin 192.168.2.1

% Connection refused by remote host
SERVER>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Request timed out.
```

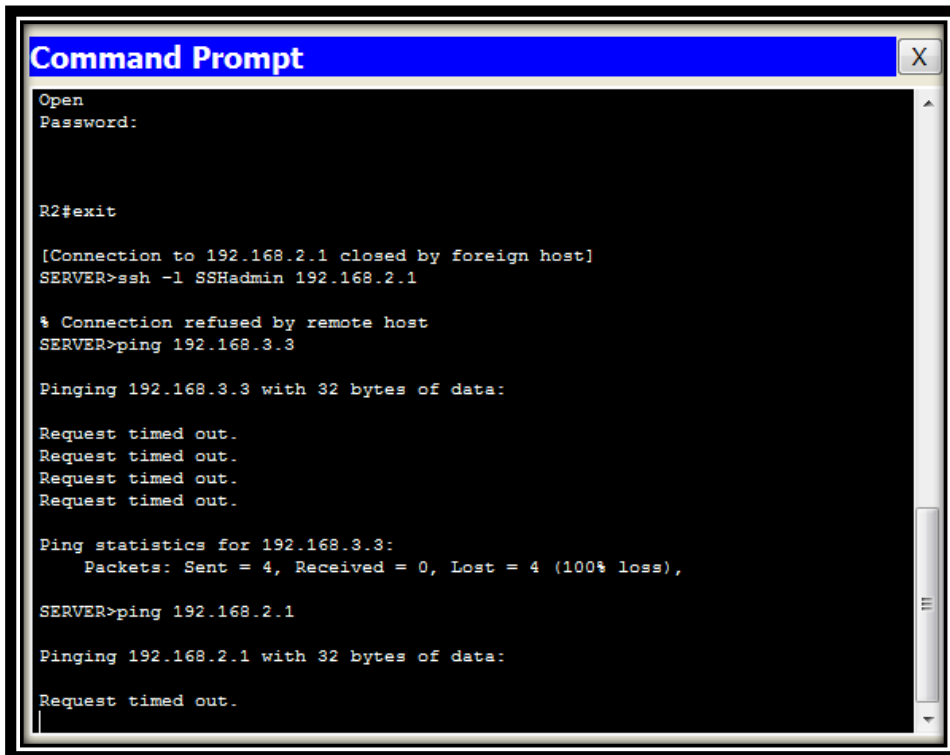
Step 2: Make any necessary changes to ACL 120 to permit and deny the specified traffic.

Use the **access-list** command to create a numbered IP ACL.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Step 3: Verify that PC-A can successfully ping the loopback interface on R2.



```
Command Prompt
Open
Password:

R2#exit

[Connection to 192.168.2.1 closed by foreign host]
SERVER>ssh -l SSHadmin 192.168.2.1

% Connection refused by remote host
SERVER>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

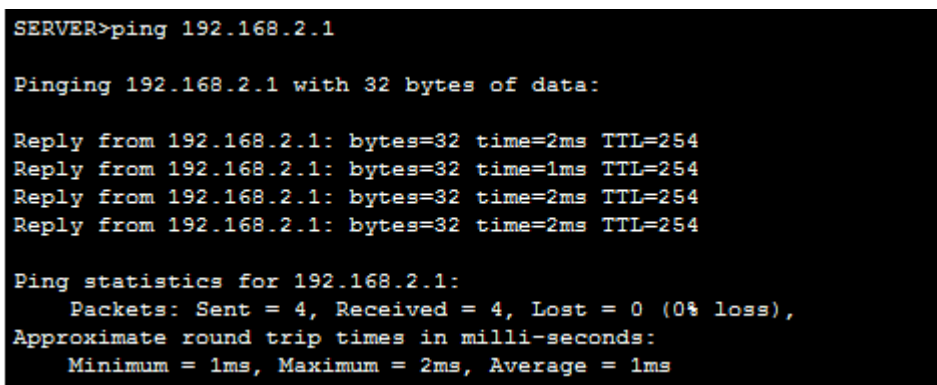
Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

SERVER>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Request timed out.
```

Despues de reconfigurar queda ok



```
SERVER>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=2ms TTL=254
Reply from 192.168.2.1: bytes=32 time=1ms TTL=254
Reply from 192.168.2.1: bytes=32 time=2ms TTL=254
Reply from 192.168.2.1: bytes=32 time=2ms TTL=254

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Part 5: Create a Numbered IP ACL 110 on R3

Deny all outbound packets with source address outside the range of internal IP

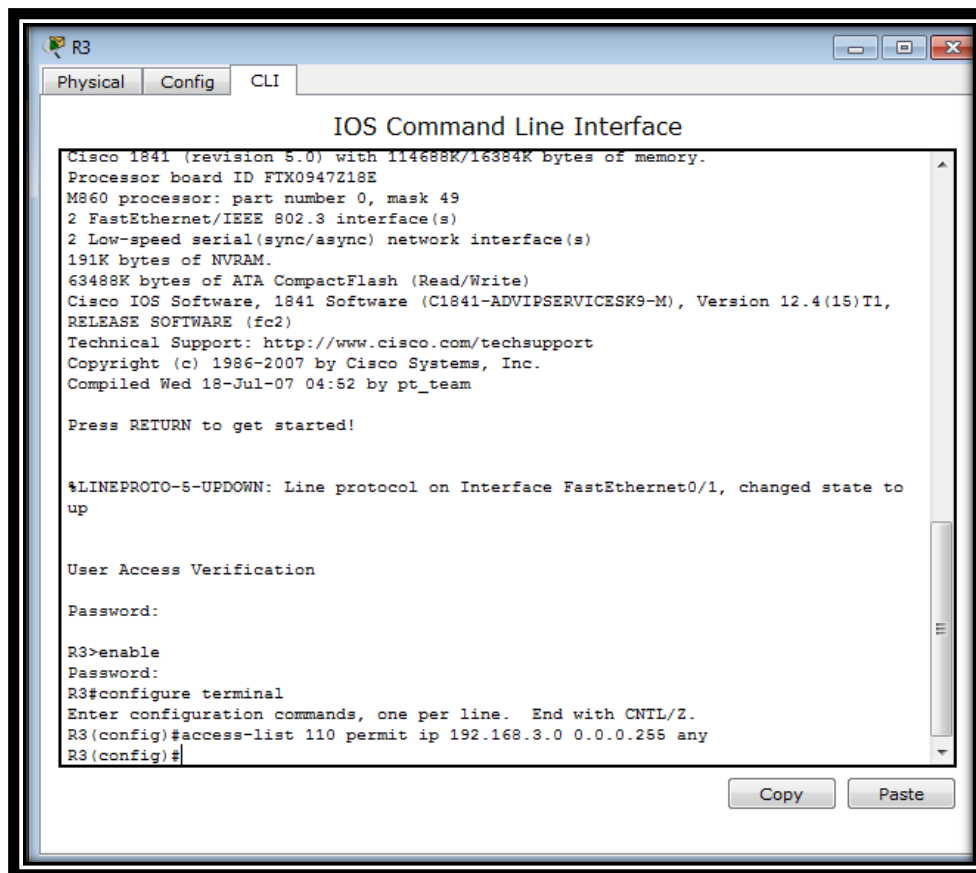
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



addresses on R3.

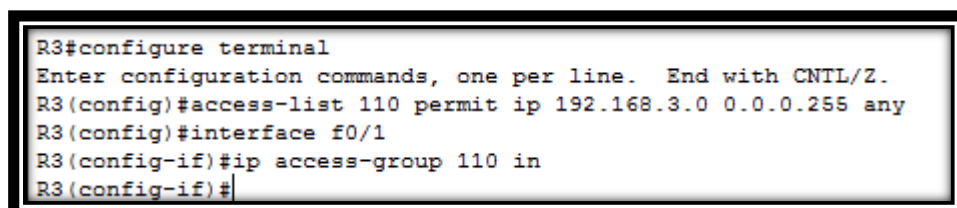
Step 1: Configure ACL 110 to permit only traffic from the inside network.

Use the **access-list** command to create a numbered IP ACL.



Step 2: Apply the ACL to interface F0/1.

Use the **ip access-group** command to apply the access list to incoming traffic on interface F0/1.



UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Part 6: Create a Numbered IP ACL 100 on R3

On **R3**, block all packets containing the source IP address from the following pool of addresses: 127.0.0.0/8, any RFC 1918 private addresses, and any IP multicast address.

Step 1: Configure ACL 100 to block all specified traffic from the outside network.

You should also block traffic sourced from your own internal address space if it is not an RFC 1918 address (in this activity, your internal address space is part of the private address space specified in RFC 1918).

Use the **access-list** command to create a numbered IP ACL.

```
R3(config-if)#exit
R3(config)#access-list 100 permit tcp 10.0.0.0 0.255.255.255 eq 22 host
192.168.3.3
R3(config)#access-list deny ip 10.0.0.0 0.255.255.255 any
^
% Invalid input detected at '^' marker.

R3(config)#access-list 100 deny ip 10.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 172.16.0.0 0.15.22.255 any
R3(config)#access-list 100 deny ip 192.168.0.0 0.0.255.255 any
R3(config)#access-list 100 deny ip 127.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 224.0.0.0 15.255.255.255 any
R3(config)#access-list 100 permit ip any any
R3(config)#
```

Step 2: Apply the ACL to interface Serial 0/0/1.

Use the **ip access-group** command to apply the access list to incoming traffic on interface Serial 0/0/1.

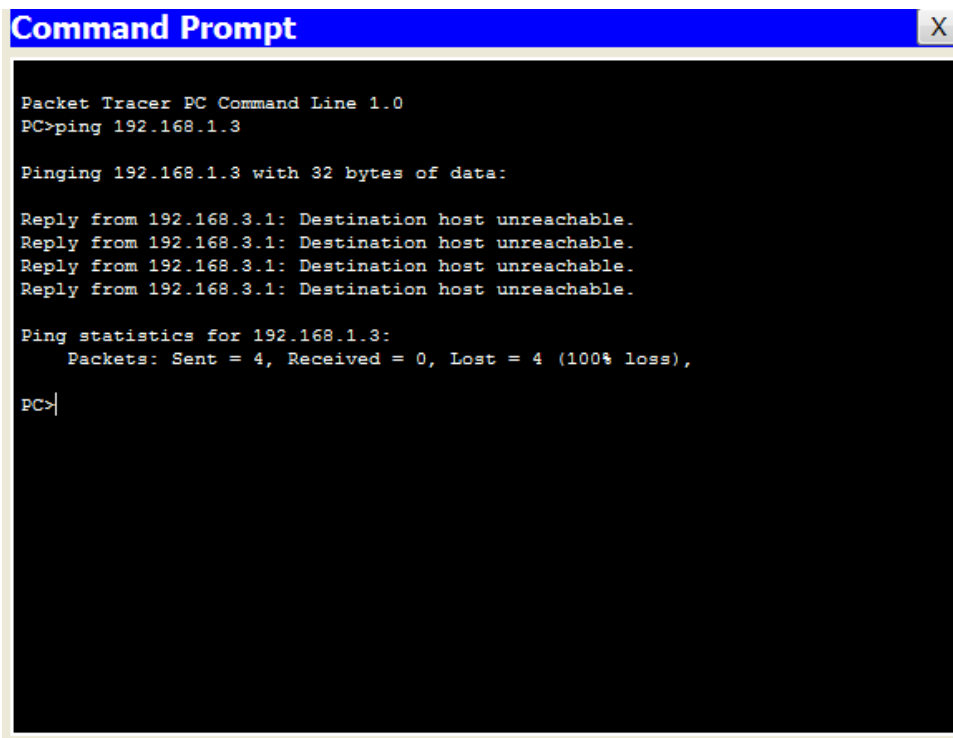
```
R3(config)#access-list 100 deny ip 172.16.0.0 0.15.22.255 any
R3(config)#access-list 100 deny ip 192.168.0.0 0.0.255.255 any
R3(config)#access-list 100 deny ip 127.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 224.0.0.0 15.255.255.255 any
R3(config)#access-list 100 permit ip any any
R3(config)#interface s0/0/1
R3(config-if)#ip access-group 100 in
R3(config-if)#
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Step 3: Confirm that the specified traffic entering interface Serial 0/0/1 is dropped.

From the **PC-C** command prompt, ping the **PC-A** server. The ICMP echo *replies* are blocked by the ACL since they are sourced from the 192.168.0.0/16 address space.



```
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

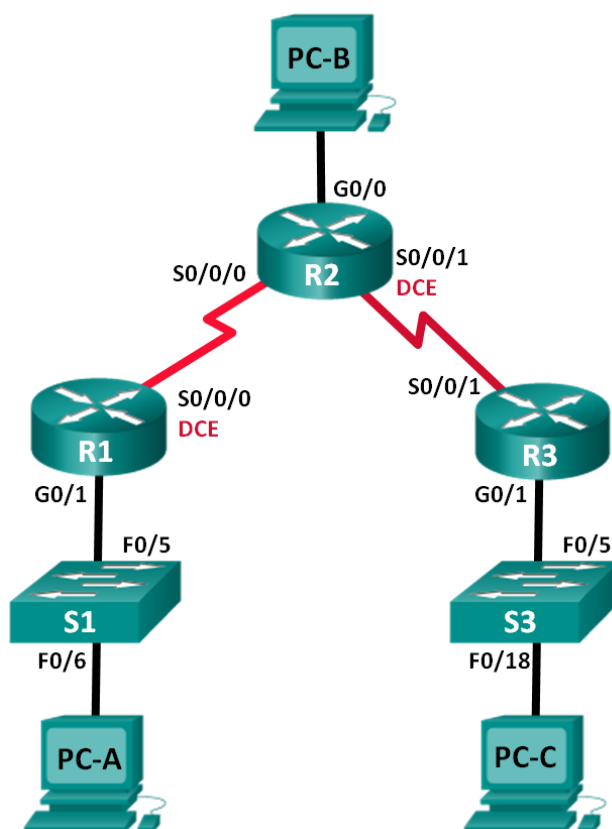
Step 4: Check results.

Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

Laboratorio 7.3.2.4 Packet Tracer - configuración básica de RIPv2 y RIPvng

Topología



UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



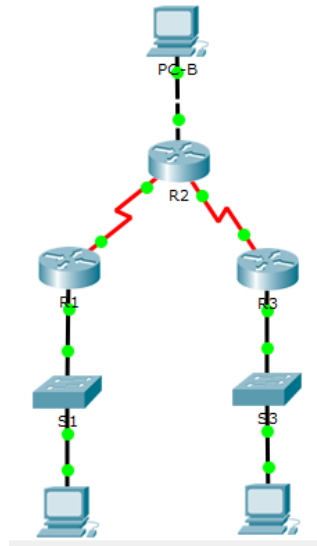
Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	172.30.10.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	G0/0	209.165.201.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
R3	G0/1	172.30.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	N/A	VLAN 1	N/A	N/A
S3	N/A	VLAN 1	N/A	N/A
PC-A	NIC	172.30.10.3	255.255.255.0	172.30.10.1
PC-B	NIC	209.165.201.2	255.255.255.0	209.165.201.1
PC-C	NIC	172.30.30.3	255.255.255.0	172.30.30.1

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
En la parte 1, establecerá la topología de la red y configurará los parámetros básicos.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

Paso 1. realizar el cableado de red tal como se muestra en la topología.



Paso 2. inicializar y volver a cargar el router y el switch.

Paso 3. configurar los parámetros básicos para cada router y switch.

- Desactive la búsqueda del DNS.
- Configure los nombres de los dispositivos como se muestra en la topología.
- Configurar la encriptación de contraseñas.
- Asigne **class** como la contraseña del modo EXEC privilegiado.
- Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.
- Configure **logging synchronous** para la línea de consola.
- Configure la dirección IP que se indica en la tabla de direccionamiento para todas las interfaces.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Configuración R2

```

R2
Physical Config CLI Attributes
IOS Command Line Interface
Router>enable
Router#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#banner motd "Acceso solo a personal autorizado"
R2(config)#interface g0/0
R2(config-if)#ip address 209.165.201.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface s0/0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface s0/0/1
R2(config-if)#ip address 10.2.2.2 255.255.255.252
R2(config-if)#clock rate 120000
Unknown clock rate
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
R2#
  
```

Configuración R1

```

R1
Physical Config CLI Attributes
IOS Command Line Interface
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd "Acceso solo a personal autorizado"
R1(config)#interface g0/1
R1(config-if)#ip address 172.30.10.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface s0/0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#clock rate 120000
Unknown clock rate
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
  
```

Configuración R3

Configuración S1

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



R3

Physical Config CLI Attributes

IOS Command Line Interface

```

Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line vty 0 15
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#banner motd "Acceso solo a personal autorizado"
R3(config-if)#ip address 172.30.30.1 255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface s0/0/1
R3(config-if)#ip address 10.2.2.1 255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface g0/1
R3(config-if)#ip address 172.30.30.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config-if)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#cop r s
          
```

S1

Physical Config CLI Attributes

IOS Command Line Interface

```

Switch>enable
Switch#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#logging synchronous
S1(config)#line console 0
S1(config-line)#logging synchronous
S1(config-line)#exit
S1(config)#banner motd "Acceso solo personal autorizado"
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#
S1#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
          
```

Configuración S3

S3

Physical Config CLI Attributes

IOS Command Line Interface

```

Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S3
S3(config)#no ip domain-lookup
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#login
S3(config-line)#logging synchronous
S3(config-line)#line vty 0 15
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd "Acceso solo personal autorizado"
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console
S3#
S3#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
S3#
          
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Paso 4. configurar los equipos host.

Consulte la tabla de direccionamiento para obtener información de direcciones de los equipos host.

PC-A

Physical	Config	Desktop	Attributes	Software/Services
IP Configuration				
IP Configuration				
<input type="radio"/> DHCP <input checked="" type="radio"/> Static				
IP Address: 172.30.10.3				
Subnet Mask: 255.255.255.0				
Default Gateway: 172.30.10.1				

PC-B

Physical	Config	Desktop	Attributes	Software/Services
IP Configuration				
IP Configuration				
<input type="radio"/> DHCP <input checked="" type="radio"/> Static				
IP Address: 209.165.201.2				
Subnet Mask: 255.255.255.0				
Default Gateway: 209.165.201.1				

PC-C

Physical	Config	Desktop	Attributes	Software/Services
IP Configuration				
IP Configuration				
<input type="radio"/> DHCP <input checked="" type="radio"/> Static				
IP Address: 172.30.30.3				
Subnet Mask: 255.255.255.0				
Default Gateway: 172.30.30.1				

Paso 5. Probar la conectividad.

En este momento, las computadoras no pueden hacerse ping entre sí.

- Cada estación de trabajo debe tener capacidad para hacer ping al router conectado. Verifique y resuelva los problemas, si es necesario.

PC-A

```

Packet Tracer PC Command Line 1.0
C:\>ping 172.30.10.1

Pinging 172.30.10.1 with 32 bytes of data:

Reply from 172.30.10.1: bytes=32 time=35ms TTL=255
Reply from 172.30.10.1: bytes=32 time<1ms TTL=255
Reply from 172.30.10.1: bytes=32 time<1ms TTL=255
Reply from 172.30.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.30.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 35ms, Average = 8ms
          
```

PC-B

```

Packet Tracer PC Command Line 1.0
C:\>ping 209.165.201.1

Pinging 209.165.201.1 with 32 bytes of data:

Reply from 209.165.201.1: bytes=32 time=1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
          
```

PC-C

```

Packet Tracer PC Command Line 1.0
C:\>ping 172.30.30.1

Pinging 172.30.30.1 with 32 bytes of data:

Reply from 172.30.30.1: bytes=32 time=1ms TTL=255
Reply from 172.30.30.1: bytes=32 time<1ms TTL=255
Reply from 172.30.30.1: bytes=32 time<1ms TTL=255
Reply from 172.30.30.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.30.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
          
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



- b. Los routers deben poder hacerse ping entre sí. Verifique y resuelva los problemas, si es necesario.

```
R2>ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/7/32 ms

R2>ping 10.2.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/6/27 ms
```

Ping R2 a R1 y R2 a R3

Parte 2: configurar y verificar el routing RIPv2

En la parte 2, configurará el routing RIPv2 en todos los routers de la red y, luego, verificará que las tablas de routing se hayan actualizado correctamente. Una vez que haya verificado RIPv2, deshabilitará el resumen automático, configurará una ruta predeterminada y verificará la conectividad de extremo a extremo.

Paso 1. Configurar el enrutamiento RIPv2.

- a. En el R1, configure RIPv2 como el protocolo de routing y anuncie las redes correspondientes.

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#passive-interface g0/1
R1(config-router)#network 172.30.0.0
R1(config-router)#network 10.0.0.0
```

El comando **passive-interface** evita que las actualizaciones de routing se envíen a través de la interfaz especificada. Este proceso evita tráfico de routing innecesario en la LAN. Sin embargo, la red a la que pertenece la interfaz especificada aún se anuncia en las actualizaciones de routing enviadas por otras interfaces.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



- b. Configure RIPv2 en el R3 y utilice la instrucción **network** para agregar las redes apropiadas y evitar actualizaciones de routing en la interfaz LAN.

```
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#passive-interface g0/1
R3(config-router)#network 172.30.0.0
R3(config-router)#network 10.0.0.0
```

- c. Configure RIPv2 en el R2. No anuncie la red 209.165.201.0.

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 10.0.0.0
R2(config-router)#exit
```

Nota: no es necesario establecer la interfaz G0/0 como pasiva en el R2, porque la red asociada a esta interfaz no se está anunciando.

Paso 2. examinar el estado actual de la red.

- a. Se pueden verificar los dos enlaces seriales rápidamente mediante el comando **show ip interface brief** en R2.

```
R2#show ip interface brief
Interface          IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0 209.165.201.1   YES manual up
up
GigabitEthernet0/1 unassigned      YES unset
administratively down down
Serial0/0/0         10.1.1.2        YES manual up
up
Serial0/0/1         10.2.2.2        YES manual up
up
Vlan1               unassigned      YES unset
administratively down down
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



b. Verifique la conectividad entre las computadoras.

PC-A

```
Physical Config Desktop Attributes Software/Services
Command Prompt
C:\>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.

Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

¿Es posible hacer ping de la PC-A a la PC-B? R/ No ¿Por qué? R/ Porque el R1 y R2 NO están intercambiando información acerca de esa red. No participa en RIP.

PC-A

```
Physical Config Desktop Attributes Software/Services
Command Prompt
C:\>ping 172.30.30.3

Pinging 172.30.30.3 with 32 bytes of data:

Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.

Ping statistics for 172.30.30.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

¿Es posible hacer ping de la PC-A a la PC-C? R/ No ¿Por qué? R/ R1 y R3 no tienen ruta hacia la subred específica en el router remoto

PC-C

```
Physical Config Desktop Attributes Software/Services
Command Prompt
C:\>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.

Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

¿Es posible hacer ping de la PC-C a la PC-B? R/ No ¿Por qué? R/ Porque la G0/0 de R2 no participa en RIP

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



¿Es posible hacer ping de la PC-C a la PC-A? No ¿Por qué? Por la misma razón del ping fallido de PC-A a PC-C

- c. Verifique que RIPv2 se ejecute en los routers.

Puede usar los comandos **debug ip rip**, **show ip protocols** y **show run** para confirmar que RIPv2 esté en ejecución. A continuación, se muestra el resultado del comando **show ip protocols** para el R1.

```
R1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 4 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface          Send Recv Triggered RIP Key-chain
  Serial0/0/0         2      2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
  172.30.0.0
Passive Interface(s):
  GigabitEthernet0/1
Routing Information Sources:
  Gateway         Distance      Last Update
  10.1.1.2         120           00:00:24
Distance: (default is 120)
```

Al emitir el comando **debug ip rip** en el R2, ¿qué información se proporciona que confirma que RIPv2 está en ejecución? R/ Se envía la actualización 224.0.0.9 vía serial 0/0/0 y vía serial 0/0/1

```
R2#debug ip rip
RIP protocol debugging is on
R2#RIP: received v2 update from 10.2.2.1 on Serial0/0/1
  172.30.0.0/16 via 0.0.0.0 in 1 hops
RIP: received v2 update from 10.1.1.1 on Serial0/0/0
  172.30.0.0/16 via 0.0.0.0 in 1 hops
RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
  10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
  10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
```

Cuando haya terminado de observar los resultados de la depuración, emita el comando **undebug all** en la petición de entrada del modo EXEC privilegiado.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Al emitir el comando **show run** en el R3, ¿qué información se proporciona que confirma que RIPv2 está en ejecución?

```
Router rip
versión 2
Passive-interface GigabitEthernet0/1
Network 10.0.0.0
Network 172.30.0.0
```

```
router rip
version 2
passive-interface GigabitEthernet0/1
network 10.0.0.0
network 172.30.0.0
```

- d. Examinar el sumarización automática de las rutas.

Las LAN conectadas al R1 y el R3 se componen de redes no contiguas. El R2 muestra dos rutas de igual costo a la red 172.30.0.0/16 en la tabla de routing. El R2 solo muestra la dirección de red principal con clase 172.30.0.0 y no muestra ninguna de las subredes de esta red. Use el comando R2# **show ip route**.

```
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C    10.1.1.0/30 is directly connected, Serial0/0/0
L    10.1.1.2/32 is directly connected, Serial0/0/0
C    10.2.2.0/30 is directly connected, Serial0/0/1
L    10.2.2.2/32 is directly connected, Serial0/0/1
R    172.30.0.0/16 [120/1] via 10.2.2.1, 00:00:02, Serial0/0/1
      [120/1] via 10.1.1.1, 00:00:05, Serial0/0/0
209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.201.0/24 is directly connected,
GigabitEthernet0/0
L    209.165.201.1/32 is directly connected,
GigabitEthernet0/0
```

El R1 solo muestra sus propias subredes para la red 172.30.0.0. El R1 no tiene ninguna ruta para las subredes 172.30.0.0 en el R3. Use el comando R1# **show ip route**

```
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C    10.1.1.0/30 is directly connected, Serial0/0/0
L    10.1.1.1/32 is directly connected, Serial0/0/0
R    10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:03, Serial0/0/0
172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.30.10.0/24 is directly connected, GigabitEthernet0/1
L    172.30.10.1/32 is directly connected, GigabitEthernet0/1
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



El R3 solo muestra sus propias subredes para la red 172.30.0.0. El R3 no tiene ninguna ruta para las subredes 172.30.0.0 en el R1. Use el comando R3# **show ip route**

```

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R   10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:18, Serial0/0/1
C   10.2.2.0/30 is directly connected, Serial0/0/1
L   10.2.2.1/32 is directly connected, Serial0/0/1
172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C   172.30.30.0/24 is directly connected, GigabitEthernet0/1
L   172.30.30.1/32 is directly connected, GigabitEthernet0/1

```

Utilice el comando **debug ip rip** en el R2 para determinar las rutas recibidas en las actualizaciones RIP del R3 e indíquelas a continuación.

received v2 update from 10.1.1.1 on Serial0/0/0
received v2 update from 10.2.2.1 on Serial0/0/1

```

R2#debug ip rip
RIP protocol debugging is on
R2#RIP: received v2 update from 10.2.2.1 on Serial0/0/1
      172.30.0.0/16 via 0.0.0.0 in 1 hops
RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
      10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
      10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
RIP: received v2 update from 10.1.1.1 on Serial0/0/0
      172.30.0.0/16 via 0.0.0.0 in 1 hops
RIP: received v2 update from 10.2.2.1 on Serial0/0/1

```

El R3 no está envía ninguna de las subredes 172.30.0.0, solo la ruta resumida 172.30.0.0/16, incluida la máscara de subred. Por lo tanto, las tablas de routing del R1 y el R2 no muestran las subredes 172.30.0.0 en el R3.

Paso 1. Desactivar la sumarización automática.

- El comando **no auto-summary** se utiliza para desactivar la sumarización automática en RIPv2. Deshabilite la sumarización automática en todos los routers. Los routers ya no resumirán las rutas en los límites de las redes principales con clase. Aquí se muestra R1 como ejemplo.

R1(config)# **router rip**

R1(config-router)# **no auto-summary**

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



- b. Emita el comando **clear ip route *** para borrar la tabla de routing.

R1(config-router)# end

R1# clear ip route *

```
R1(config)#router rip
R1(config-router)#no auto-summary
R1(config-router)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#clear ip route *

R2(config)#router rip
R2(config-router)#no auto-summary
R2(config-router)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

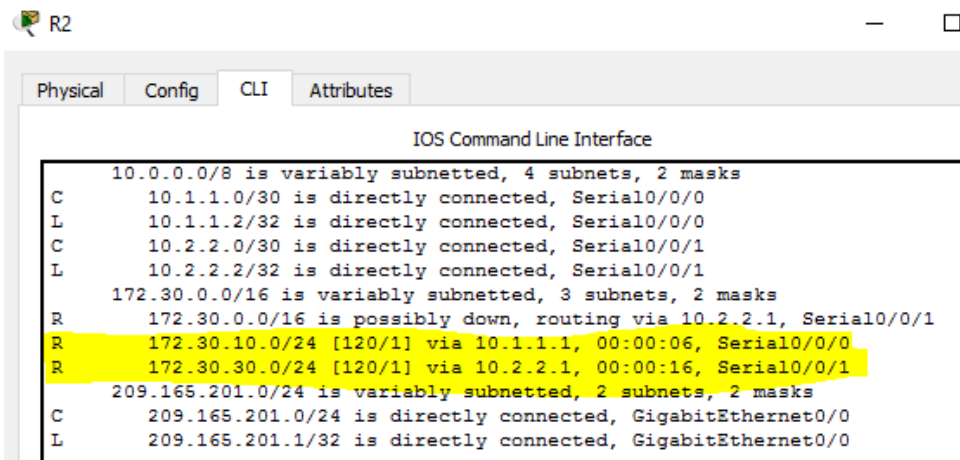
R2#clear ip route *

R3(config)#router rip
R3(config-router)#no auto-summary
R3(config-router)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#clear ip route *
```

- c. Examinar las tablas de enrutamiento Recuerde que la convergencia de las tablas de routing demora un tiempo después de borrarlas.

Las subredes LAN conectadas al R1 y el R3 ahora deberían aparecer en las tres tablas de routing.



R1# show ip route

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



R1

Physical Config CLI Attributes

IOS Command Line Interface

```

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C    10.1.1.0/30 is directly connected, Serial0/0/0
L    10.1.1.1/32 is directly connected, Serial0/0/0
R    10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:15, Serial0/0/0
    172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
C    172.30.10.0/24 is directly connected, GigabitEthernet0/1
L    172.30.10.1/32 is directly connected, GigabitEthernet0/1
R    172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:15, Serial0/0/0
  
```

R3# show ip route

R3

Physical Config CLI Attributes

IOS Command Line Interface

```

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R    10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:19, Serial0/0/1
C    10.2.2.0/30 is directly connected, Serial0/0/1
L    10.2.2.1/32 is directly connected, Serial0/0/1
    172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
R    172.30.10.0/24 [120/2] via 10.2.2.2, 00:00:19, Serial0/0/1
C    172.30.30.0/24 is directly connected, GigabitEthernet0/1
L    172.30.30.1/32 is directly connected, GigabitEthernet0/1
  
```

d. Utilice el comando **debug ip rip** en el R2 para examinar las actualizaciones RIP.

R2# debug ip rip

```

R2#debug ip rip
RIP protocol debugging is on
R2#RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
    10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
    172.30.10.0/24 via 0.0.0.0, metric 2, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
    10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
    172.30.30.0/24 via 0.0.0.0, metric 2, tag 0
RIP: received v2 update from 10.1.1.1 on Serial0/0/0
    172.30.10.0/24 via 0.0.0.0 in 1 hops
RIP: received v2 update from 10.2.2.1 on Serial0/0/1
    172.30.30.0/24 via 0.0.0.0 in 1 hops
  
```

Después de 60 segundos, emita el comando **no debug ip rip**.

¿Qué rutas que se reciben del R3 se encuentran en las actualizaciones RIP?

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



R/ 172.30.30.0/24

¿Se incluyen ahora las máscaras de las subredes en las actualizaciones de enrutamiento?

R/ Si

Paso 2. Configure y redistribuya una ruta predeterminada para el acceso a Internet.

- Desde el R2, cree una ruta estática a la red 0.0.0.0 0.0.0.0, con el comando **ip route**. Esto envía todo tráfico de dirección de destino desconocida a la interfaz G0/0 del R2 hacia la PC-B y simula Internet al establecer un gateway de último recurso en el router R2.

```
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.2
```

- El R2 anunciará una ruta a los otros routers si se agrega el comando **default-information originate** a la configuración de RIP.

```
R2(config)# router rip
```

```
R2(config-router)# default-information originate
```

```
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.2
R2(config)#router rip
R2(config-router)#default-information originate
R2(config-router)#end
```

Paso 3. Verificar la configuración de enrutamiento.

- Consulte la tabla de routing en el R1.

```
Gateway of last resort is 10.1.1.2 to network 0.0.0.0
  10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C    10.1.1.0/30 is directly connected, Serial0/0/0
L    10.1.1.1/32 is directly connected, Serial0/0/0
R    10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:20, Serial0/0/0
  172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
C    172.30.10.0/24 is directly connected, GigabitEthernet0/1
L    172.30.10.1/32 is directly connected, GigabitEthernet0/1
R    172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:20, Serial0/0/0
R*   0.0.0.0/0 [120/1] via 10.1.1.2, 00:00:20, Serial0/0/0
```

¿Cómo se puede saber, a partir de la tabla de routing, que la red dividida en subredes que comparten el R1 y el R3 tiene una ruta para el tráfico de Internet?

R/ Porque hay una puerta de enlace o Gateway de último recurso que nos conecta a internet.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



- b. Consulte la tabla de routing en el R2.

```
Gateway of last resort is 209.165.201.2 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C    10.1.1.0/30 is directly connected, Serial0/0/0
L    10.1.1.2/32 is directly connected, Serial0/0/0
C    10.2.2.0/30 is directly connected, Serial0/0/1
L    10.2.2.2/32 is directly connected, Serial0/0/1
L    172.30.0.0/24 is subnetted, 2 subnets
R    172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:27, Serial0/0/0
R    172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:22, Serial0/0/1
C    209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.201.0/24 is directly connected, GigabitEthernet0/0
L    209.165.201.1/32 is directly connected, GigabitEthernet0/0
S*   0.0.0.0/0 [1/0] via 209.165.201.2
```

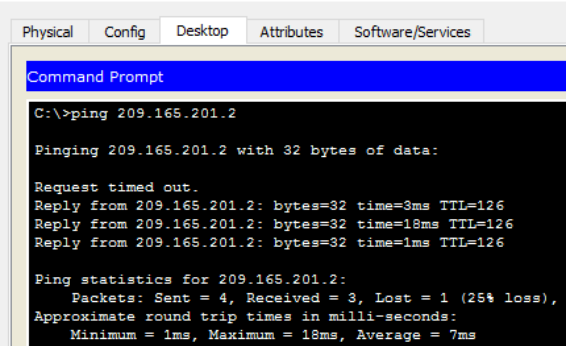
¿En qué forma se proporciona la ruta para el tráfico de Internet en la tabla de routing?

R/ En que se relaciona la sub red creada para la dirección de internet 209.165.201.2.

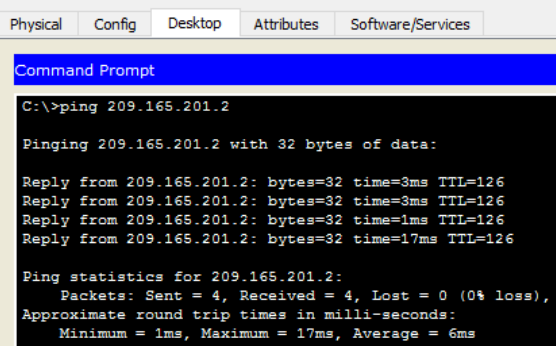
Paso 4. Verifique la conectividad.

- a. Simule el envío de tráfico a Internet haciendo ping de la PC-A y la PC-C a 209.165.201.2.

PC-A



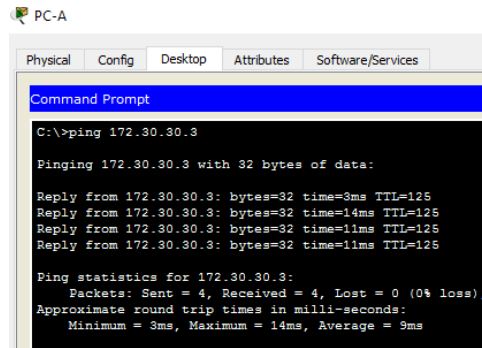
PC-C



¿Tuvieron éxito los pings? Si

- b. Verifique que los hosts dentro de la red dividida en subredes tengan posibilidad de conexión entre sí haciendo ping entre la PC-A y la PC-C.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
PC-A
Physical Config Desktop Attributes Software/Services
Command Prompt
C:\>ping 172.30.30.3

Pinging 172.30.30.3 with 32 bytes of data:

Reply from 172.30.30.3: bytes=32 time=3ms TTL=125
Reply from 172.30.30.3: bytes=32 time=14ms TTL=125
Reply from 172.30.30.3: bytes=32 time=11ms TTL=125
Reply from 172.30.30.3: bytes=32 time=11ms TTL=125

Ping statistics for 172.30.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 14ms, Average = 9ms
```

¿Tuvieron éxito los pings? Si

Nota: quizá sea necesario deshabilitar el firewall de las computadoras.

Parte 3: configurar IPv6 en los dispositivos

En la parte 3, configurará todas las interfaces con direcciones IPv6 y verificará la conectividad.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv6/longitud de prefijo	Gateway predeterminado
R1	G0/1	2001:DB8:ACAD:A::1/64 FE80::1 link-local	No aplicable
	S0/0/0	2001:DB8:ACAD:12::1/64 FE80::1 link-local	No aplicable
R2	G0/0	2001:DB8:ACAD:B::2/64 FE80::2 link-local	No aplicable
	S0/0/0	2001:DB8:ACAD:12::2/64 FE80::2 link-local	No aplicable
	S0/0/1	2001:DB8:ACAD:23::2/64 FE80::2 link-local	No aplicable
R3	G0/1	2001:DB8:ACAD:C::3/64 FE80::3 link-local	No aplicable
	S0/0/1	2001:DB8:ACAD:23::3/64 FE80::3 link-local	No aplicable
PC-A	NIC	2001:DB8:ACAD:A::A/64	FE80::1
PC-B	NIC	2001:DB8:ACAD:B::B/64	FE80::2
PC-C	NIC	2001:DB8:ACAD:C::C/64	FE80::3

Paso 1. configurar los equipos host.

Consulte la tabla de direccionamiento para obtener información de direcciones de los equipos host.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



PC-A

Physical Config Desktop Attributes Software/Services

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IP Address 172.30.10.3

Subnet Mask 255.255.255.0

Default Gateway 172.30.10.1

DNS Server

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address 2001:DB8:ACAD:A::A / 64

Link Local Address FE80::2E0:B0FF:FE84:864B

IPv6 Gateway FE80::1

PC-B

Physical Config Desktop Attributes Software/Services

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IP Address 209.165.201.2

Subnet Mask 255.255.255.0

Default Gateway 209.165.201.1

DNS Server

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address 2001:DB8:ACAD:B::B / 64

Link Local Address FE80::207:ECFF:FE25:9D74

IPv6 Gateway FE80::2

PC-C

Physical Config Desktop Attributes Software/Services

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IP Address 172.30.30.3

Subnet Mask 255.255.255.0

Default Gateway 172.30.30.1

DNS Server

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address 2001:DB8:ACAD:C::C / 64

Link Local Address FE80::260:47FF:FE72:4C63

IPv6 Gateway FE80::3

Paso 2. configurar IPv6 en los routers.

Nota: la asignación de una dirección IPv6 además de una dirección IPv4 en una interfaz se conoce como “dual-stacking” (o apilamiento doble). Esto se debe a que las pilas de protocolos IPv4 e IPv6 están activas.

- Para cada interfaz del router, asigne la dirección global y la dirección link local de la tabla de direccionamiento.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



b. Habilite el routing IPv6 en cada router.

Direccionamiento R1

```
R1(config)#interface g0/1
R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shutdown
R1(config-if)#interface s0/0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:12::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shutdown
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 unicast-routing
R1(config)#exit
```

Direccionamiento R2:

```
R2(config)#interface g0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:B::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#no shutdown
R2(config-if)#interface s0/0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:12::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#no shutdown
R2(config-if)#interface s0/0/1
R2(config-if)#ipv6 address 2001:DB8:ACAD:23::2/64
R2(config-if)#ipv6 address FE80::2 link local
R2(config-if)#exit
R2#

% Invalid input detected at '^' marker.

R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#ipv6 unicast-routing
R2(config)#exit
R2#
```

Direccionamiento R3:

```
R3(config)#interface g0/1
R3(config-if)#ipv6 address 2001:DB8:ACAD:C::3/64
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#no shutdown
R3(config-if)#interface s0/0/1
R3(config-if)#ipv6 address 2001:DB8:ACAD:23::3/64
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#ipv6 unicast-routing
R3(config)#exit
R3#
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



- c. Introduzca el comando apropiado para verificar las direcciones IPv6 y el estado de enlace. Escriba el comando en el espacio que se incluye a continuación.

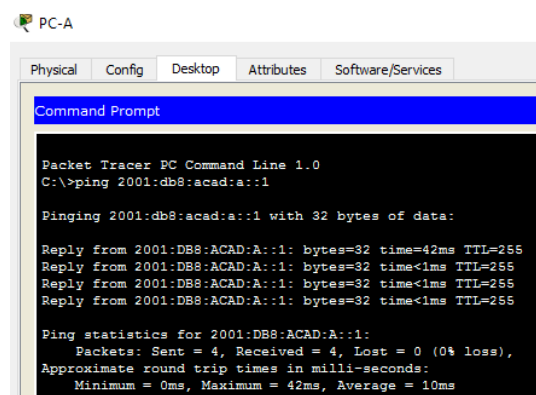
Show ipv6 interface

- d. Cada estación de trabajo debe tener capacidad para hacer ping al router conectado. Verifique y resuelva los problemas, si es necesario.

Ping PCA a R1

Ping PCB a R2

PC-A



```

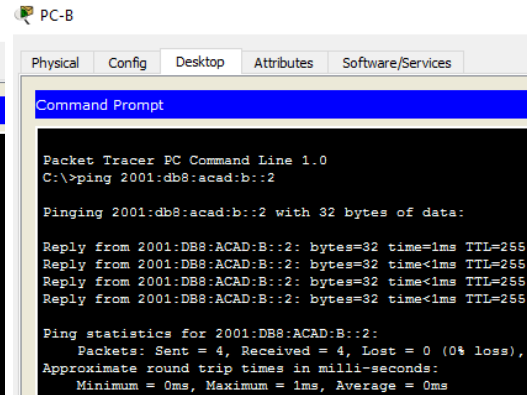
Packet Tracer PC Command Line 1.0
C:\>ping 2001:db8:acad:a::1

Pinging 2001:db8:acad:a::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:A::1: bytes=32 time=42ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 42ms, Average = 10ms
        
```

PC-B



```

Packet Tracer PC Command Line 1.0
C:\>ping 2001:db8:acad:b::2

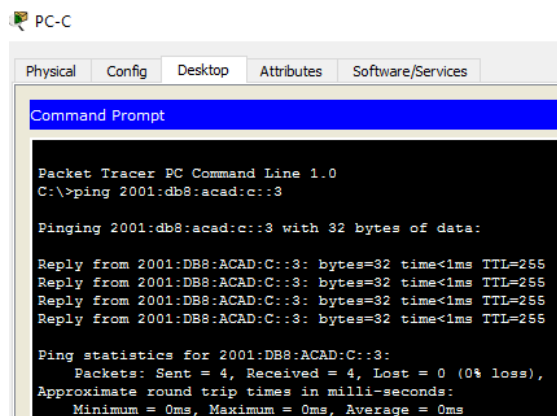
Pinging 2001:db8:acad:b::2 with 32 bytes of data:

Reply from 2001:DB8:ACAD:B::2: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:B::2: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::2: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::2: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:B::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
        
```

Ping PC-C a R3

PC-C



```

Packet Tracer PC Command Line 1.0
C:\>ping 2001:db8:acad:c::3

Pinging 2001:db8:acad:c::3 with 32 bytes of data:

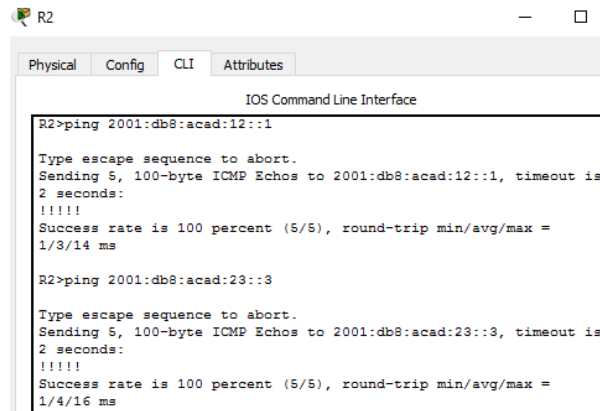
Reply from 2001:DB8:ACAD:C::3: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::3: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::3: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::3: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:C::3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
        
```

- e. Los routers deben poder hacerse ping entre sí. Verifique y resuelva los problemas, si es necesario.

Ping R2 a R1 y R2 a R3

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

```

R2>ping 2001:db8:acad:12::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:12::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/14 ms

R2>ping 2001:db8:acad:23::3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:23::3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/16 ms
  
```

Parte 4: configurar y verificar el routing RIPng

En la parte 4, configurará el routing RIPng en todos los routers, verificará que las tablas de routing estén correctamente actualizadas, configurará y distribuirá una ruta predeterminada, y verificará la conectividad de extremo a extremo.

Paso 1. configurar el routing RIPng.

- Emita el comando **ipv6 rip Test1 enable** para cada interfaz en el R1 que participará en el routing RIPng, donde **Test1** es el nombre de proceso pertinente en el nivel local.

```

R1(config)#interface g0/1
R1(config-if)#ipv6 rip Test1 enable
R1(config-if)#interface s0/0/0
R1(config-if)#ipv6 rip Test1 enable
R1(config-if)#end
  
```

- Configure RIPng para las interfaces seriales en el R2, con **Test2** como el nombre de proceso. No lo configure para la interfaz G0/0

```

R2(config)#interface s0/0/0
R2(config-if)#ipv6 rip Test2 enable
R2(config-if)#interface s0/0/1
R2(config-if)#ipv6 rip Test2 enable
R2(config-if)#end
R2#
  
```

- Configure RIPng para cada interfaz en el R3, con **Test3** como el nombre de proceso.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
R3(config)#interface g0/1
R3(config-if)#ipv6 rip Test3 enable
R3(config-if)#int s0/0/1
R3(config-if)#ipv6 rip Test3 enable
R3(config-if)#end
R3#
```

- d. Verifique que RIPng se esté ejecutando en los routers.

Los comandos **show ipv6 protocols**, **show run**, **show ipv6 rip database** y **show ipv6 rip nombre de proceso** se pueden usar para confirmar que se esté ejecutando RIPng. En el R1, emita el comando **show ipv6 protocols**.

```
R1#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip Test1"
  Interfaces:
    GigabitEthernet0/1
    Serial0/0/0
  Redistribution:
    None
```

¿En qué forma se indica RIPng en el resultado?

R/ "rip Test1"

- e. Emita el comando **show ipv6 rip Test1**.

```
R1# show ipv6 rip Test1
RIP process "Test1", port 521, multicast-group FF02::9, pid 31
  Administrative distance is 120. Maximum paths is 16
  Updates every 30 seconds, expire after 180
  Holddown lasts 0 seconds, garbage collect after 120
  Split horizon is on; poison reverse is off
  Default routes are not generated
  Periodic updates 1, trigger updates 0
  Full Advertisement 0, Delayed Events 0
  Interfaces:
    GigabitEthernet0/1
    Serial0/0/0
  Redistribution:
```

- f.

¿Cuáles son las similitudes entre RIPv2 y RIPng?

R/ La distancia administrativa es 120, Updates every 30 seconds y expire after 180 sec

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



- g. Inspecciones la tabla de routing IPv6 en cada router. Escriba el comando apropiado que se usa para ver la tabla de routing en el espacio a continuación. R/
Show ipv6 route

En el R1, ¿cuántas rutas se descubrieron mediante RIPng? R/ 2

```
R1#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS
summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 -
OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C   2001:DB8:ACAD:A::/64 [0/0]
    via GigabitEthernet0/1, directly connected
L   2001:DB8:ACAD:A::1/128 [0/0]
    via GigabitEthernet0/1, receive
R   2001:DB8:ACAD:C::/64 [120/3]
    via FE80::2, Serial0/0/0
C   2001:DB8:ACAD:12::/64 [0/0]
    via Serial0/0/0, directly connected
L   2001:DB8:ACAD:12::1/128 [0/0]
    via Serial0/0/0, receive
R   2001:DB8:ACAD:23::/64 [120/2]
    via FE80::2, Serial0/0/0
L   FF00::/8 [0/0]
    via Null0, receive
```

En el R2, ¿cuántas rutas se descubrieron mediante RIPng? R/ 2

```
R2#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS
summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 -
OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
R   2001:DB8:ACAD:A::/64 [120/2]
    via FE80::1, Serial0/0/0
C   2001:DB8:ACAD:B::/64 [0/0]
    via GigabitEthernet0/0, directly connected
L   2001:DB8:ACAD:B::2/128 [0/0]
    via GigabitEthernet0/0, receive
R   2001:DB8:ACAD:C::/64 [120/2]
    via FE80::3, Serial0/0/1
C   2001:DB8:ACAD:12::/64 [0/0]
    via Serial0/0/0, directly connected
L   2001:DB8:ACAD:12::2/128 [0/0]
    via Serial0/0/0, receive
C   2001:DB8:ACAD:23::/64 [0/0]
    via Serial0/0/1, directly connected
L   2001:DB8:ACAD:23::2/128 [0/0]
```

En el R3, ¿cuántas rutas se descubrieron mediante RIPng? R/ 2

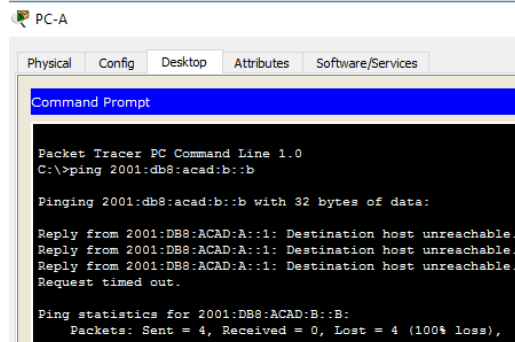
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
R3#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS
summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 -
OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
R  2001:DB8:ACAD:A::/64 [120/3]
   via FE80::2, Serial0/0/1
C  2001:DB8:ACAD:C::/64 [0/0]
   via GigabitEthernet0/1, directly connected
L  2001:DB8:ACAD:C::3/128 [0/0]
   via GigabitEthernet0/1, receive
R  2001:DB8:ACAD:12::/64 [120/2]
   via FE80::2, Serial0/0/1
C  2001:DB8:ACAD:23::/64 [0/0]
   via Serial0/0/1, directly connected
L  2001:DB8:ACAD:23::3/128 [0/0]
   via Serial0/0/1, receive
L  FF00::/8 [0/0]
   via Null0, receive
```

h. Verifique la conectividad entre las computadoras.

¿Es posible hacer ping de la PC-A a la PC-B? No



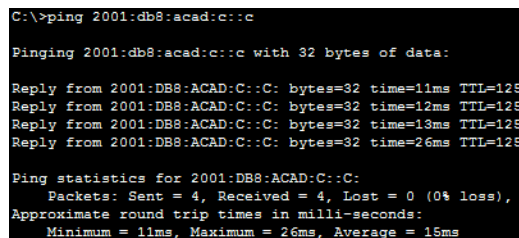
```
PC-A
Physical Config Desktop Attributes Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 2001:db8:acad:b::b

Pinging 2001:db8:acad:b::b with 32 bytes of data:

Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.
Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.
Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.
Request timed out.

Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

¿Es posible hacer ping de la PC-A a la PC-C? R/ Si



```
C:\>ping 2001:db8:acad:c::c

Pinging 2001:db8:acad:c::c with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::C: bytes=32 time=11ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=12ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=13ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=26ms TTL=125

Ping statistics for 2001:DB8:ACAD:C::C:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 26ms, Average = 15ms
```

¿Es posible hacer ping de la PC-C a la PC-B? R/ No

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
PC-C
Physical Config Desktop Attributes Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 2001:db8:acad:b::b
Pinging 2001:db8:acad:b::b with 32 bytes of data:
Reply from 2001:DB8:ACAD:C::3: Destination host unreachable.
Reply from 2001:DB8:ACAD:C::3: Destination host unreachable.
Request timed out.
Reply from 2001:DB8:ACAD:C::3: Destination host unreachable.
Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

¿Es posible hacer ping de la PC-C a la PC-A? R/ Si

```
C:\>ping 2001:db8:acad:a::a
Pinging 2001:db8:acad:a::a with 32 bytes of data:
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=12ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=13ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=12ms TTL=125
Ping statistics for 2001:DB8:ACAD:A::A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 13ms, Average = 9ms
```

¿Por qué algunos pings tuvieron éxito y otros no?

R/ Porque no hay una ruta anunciada para la red de PC-B

Paso 2. configurar y volver a distribuir una ruta predeterminada.

Desde el R2, cree una ruta estática predeterminada a la red:: 0/64 con el comando **ipv6 route** y la dirección IP de la interfaz de salida G0/0. Esto reenvía todo tráfico de dirección de destino desconocida a la interfaz G0/0 del R2 hacia la PC-B y simula Internet. Escriba el comando que utilizó en el espacio a continuación. **R/** `ipv6 route ::0/64 2001:DB8:ACAD:B::B`

```
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 route ::0/64 2001:DB8:ACAD:B::B
R2(config)#cop r s
```


UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



- a. Las rutas estáticas se pueden incluir en las actualizaciones RIPng mediante el comando **ipv6 rip nombre de proceso default-information originate** en el modo de configuración de interfaz. Configure los enlaces seriales en el R2 para enviar la ruta predeterminada en actualizaciones RIPng.

```
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface s0/0/0
R2(config-if)#ipv6 rip Test2 default-information originate
R2(config-if)#interface s0/0/1
R2(config-if)#ipv6 rip Test2 default-information originate
R2(config-if)#end
R2#
```

Paso 3. Verificar la configuración de enrutamiento.

- b. Consulte la tabla de routing IPv6 en el router R2.

```
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS
summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 -
OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S   ::/64 [1/0]
    via 2001:DB8:ACAD:B::B
R   2001:DB8:ACAD:A::/64 [120/2]
    via FE80::1, Serial0/0/0
C   2001:DB8:ACAD:B::/64 [0/0]
    via GigabitEthernet0/0, directly connected
L   2001:DB8:ACAD:B::2/128 [0/0]
    via GigabitEthernet0/0, receive
R   2001:DB8:ACAD:C::/64 [120/2]
    via FE80::3, Serial0/0/1
C   2001:DB8:ACAD:12::/64 [0/0]
    via Serial0/0/0, directly connected
L   2001:DB8:ACAD:12::2/128 [0/0]
    via Serial0/0/0, receive
C   2001:DB8:ACAD:23::/64 [0/0]
```

¿Cómo se puede saber, a partir de la tabla de routing, que el R2 tiene una ruta para el tráfico de Internet?

R/ Ya que presenta la ruta estática ::/64 por defecto

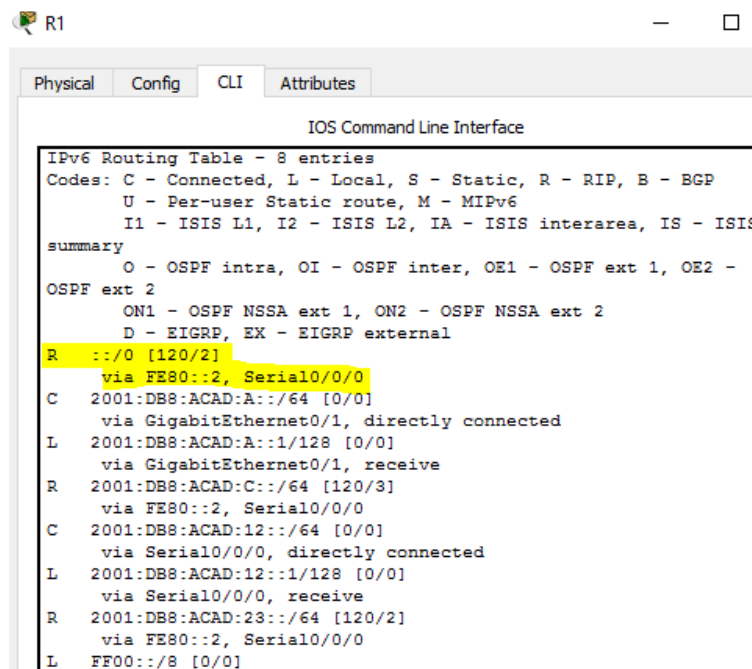
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



c. Consulte las tablas de routing del R1 y el R3.

¿Cómo se proporciona la ruta para el tráfico de Internet en sus tablas de enrutamiento?


R/ R ::/0 [120/2] via FE80::2, serial 0/0/0



```

R1
Physical Config CLI Attributes
IOS Command Line Interface
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS
summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 -
OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
R ::/0 [120/2]
  via FE80::2, Serial0/0/0
C 2001:DB8:ACAD:A::/64 [0/0]
  via GigabitEthernet0/1, directly connected
L 2001:DB8:ACAD:A::1/128 [0/0]
  via GigabitEthernet0/1, receive
R 2001:DB8:ACAD:C::/64 [120/3]
  via FE80::2, Serial0/0/0
C 2001:DB8:ACAD:12::/64 [0/0]
  via Serial0/0/0, directly connected
L 2001:DB8:ACAD:12::1/128 [0/0]
  via Serial0/0/0, receive
R 2001:DB8:ACAD:23::/64 [120/2]
  via FE80::2, Serial0/0/0
L FF00::/8 [0/0]
  
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I


 R3

Physical Config CLI Attributes

IOS Command Line Interface

```

IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS
       summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 -
       OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
R   ::/0 [120/2]
    via FE80::2, Serial0/0/1
R   2001:DB8:ACAD:A::/64 [120/3]
    via FE80::2, Serial0/0/1
C   2001:DB8:ACAD:C::/64 [0/0]
    via GigabitEthernet0/1, directly connected
L   2001:DB8:ACAD:C::3/128 [0/0]
    via GigabitEthernet0/1, receive
R   2001:DB8:ACAD:12::/64 [120/2]
    via FE80::2, Serial0/0/1
C   2001:DB8:ACAD:23::/64 [0/0]
    via Serial0/0/1, directly connected
L   2001:DB8:ACAD:23::3/128 [0/0]
    via Serial0/0/1, receive
L   FF00::/8 [0/0]
  
```

Paso 4. Verifique la conectividad.

Simule el envío de tráfico a Internet haciendo ping de la PC-A y la PC-C a 2001:DB8:ACAD:B::B/64.

¿Tuvieron éxito los pings? R/Si



Physical Config Desktop Attributes Software/Services

Command Prompt

```

Packet Tracer PC Command Line 1.0
C:\>ping 2001:db8:acad:b::b

Pinging 2001:db8:acad:b::b with 32 bytes of data:

Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=10ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126

Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 10ms, Average = 3ms
  
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



PC-C

Physical Config Desktop Attributes Software/Services

Command Prompt

```
C:\>ping 2001:db8:acad:b::b

Pinging 2001:db8:acad:b::b with 32 bytes of data:

Reply from 2001:DB8:ACAD:B::B: bytes=32 time=2ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=12ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=11ms TTL=126

Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 6ms
```

Reflexión

1. ¿Por qué desactivaría la sumarización automática para RIPv2?

R/ Para que los routers no sumaricen las rutas de acuerdo a la clase mayor

2. En ambas situaciones, ¿en qué forma descubrieron la ruta a Internet el R1 y el R3?

R/ De acuerdo a actualizaciones de rip recibidas desde el router donde fue configurada la ruta por defecto

3. ¿En qué se diferencian la configuración de RIPv2 y la de RIPv6?

R/ RIPv2 se configura identificando las redes y RIPv6 se configura en las interfaces.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet n.º 2	Interfaz serial #1	Interfaz serial n.º 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

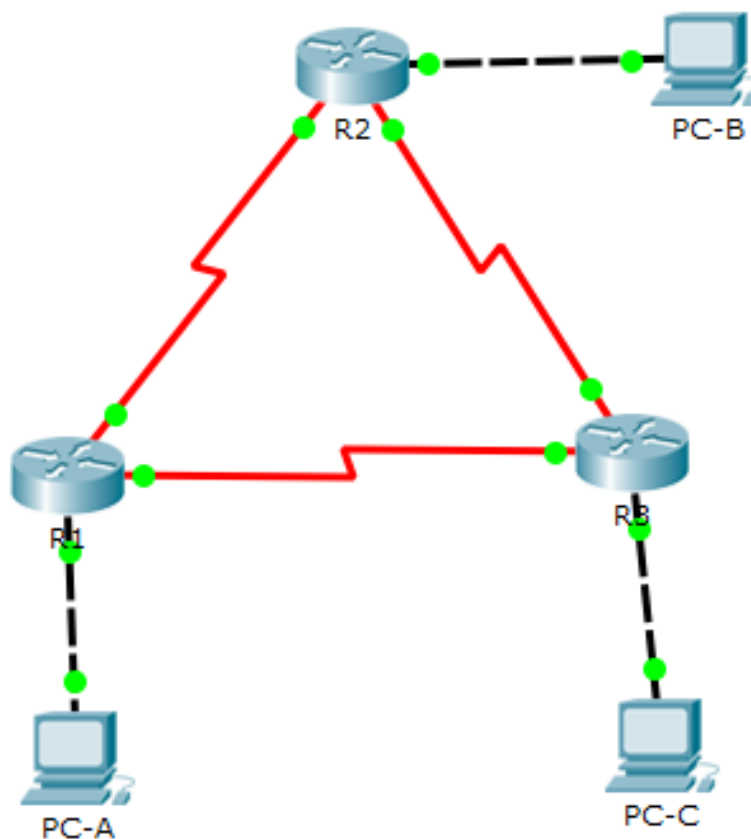
Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Laboratorio 8.2.4.5 lab - configuring basic single-area ospfv2

Topología



UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.12.1	255.255.255.252	N/A
	S0/0/1	192.168.13.1	255.255.255.252	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/0	192.168.12.2	255.255.255.252	N/A
	S0/0/1 (DCE)	192.168.23.1	255.255.255.252	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.13.2	255.255.255.252	N/A
	S0/0/1	192.168.23.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Objetivos

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

Parte 2: configurar y verificar el routing OSPF

Parte 3: cambiar las asignaciones de ID del router

Parte 4: configurar interfaces OSPF pasivas

Parte 5: cambiar las métricas de OSPF

Información básica/situación

El protocolo OSPF (Open Shortest Path First) es un protocolo de routing de estado de enlace para las redes IP. Se definió OSPFv2 para redes IPv4, y OSPFv3 para redes IPv6. OSPF detecta cambios en la topología, como fallas de enlace, y converge en una nueva estructura de routing sin bucles muy rápidamente. Computa cada ruta con el algoritmo de Dijkstra, un algoritmo SPF (Shortest Path First).

En esta práctica de laboratorio, configurará la topología de la red con routing OSPFv2, cambiará las asignaciones de ID de router, configurará interfaces pasivas, ajustará las métricas de OSPF y utilizará varios comandos de CLI para ver y verificar la información de routing OSPF.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Pueden utilizarse otros routers y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios

- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- ☐ Cables Ethernet y seriales, como se muestra en la topología

Parte . armar la red y configurar los parámetros básicos de los dispositivos

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos en los equipos host y los routers.

Step 2: realizar el cableado de red tal como se muestra en la topología.

Step 3: inicializar y volver a cargar los routers según sea necesario.

Step 4: configurar los parámetros básicos para cada router.

- a. Desactive la búsqueda del DNS.
- b. Configure el nombre del dispositivo como se muestra en la topología.
- c. Asigne **class** como la contraseña del modo EXEC privilegiado.
- d. Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- e. Configure un aviso de mensaje del día (MOTD) para advertir a los usuarios que el acceso no autorizado está prohibido.
- f. Configure **logging synchronous** para la línea de consola.
- g. Configure la dirección IP que se indica en la tabla de direccionamiento para todas las interfaces.
- h. Establezca la frecuencia de reloj para todas las interfaces seriales DCE en **128000**.
- i. Copie la configuración en ejecución en la configuración de inicio

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



IOS Command Line Interface

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int g0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R1(config-if)#int s0/0/0
R1(config-if)#ip address 192.168.12.1 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#int s0/0/
^
% Invalid input detected at '^' marker.

R1(config-if)#int s0/0/1
R1(config-if)#ip address 192.168.13.1 255.255.255.252
R1(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R1(config-if)#int s0/0/0
R1(config-if)#no shut
|
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int g0/0
Router(config-if)#ip add 192.168.2.1 255.255.255.0
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

Router(config-if)#int s0/0/0
Router(config-if)#ip add 192.168.12.2 255.255.255.252
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

Router(config-if)#int s0/0/1
Router(config-if)#ip add 192.168.2.2 255.255.255.252
% 192.168.2.0 overlaps with GigabitEthernet0/0
Router(config-if)#ip add 192.168.23.1 255.255.255.252
Router(config-if)#clock rate 128000
Router(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
Router(config-if)#
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
Router(config)#hostname R3
R3(config)#int g0/0
R3(config-if)#ip add 192.168.3.1 255.255.255.0
R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state
to up

R3(config-if)#int s0/0/0
R3(config-if)#ip add 192.168.13.2 255.255.255.252
R3(config-if)#no shut

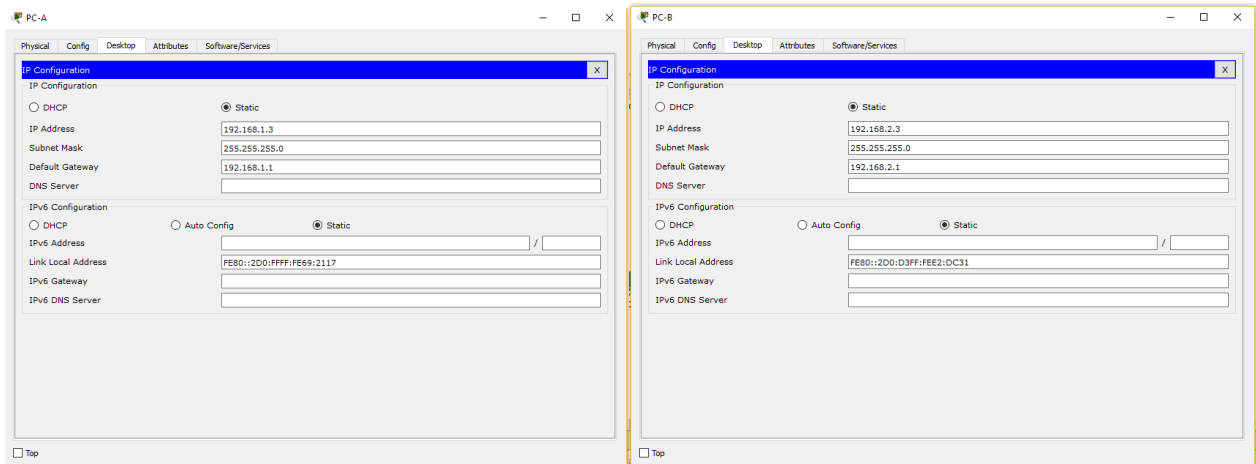
R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R3(config-if)#int s0/0/0
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
R3(config-if)#int s0/0/1
R3(config-if)#ip add 192.168.23.2 255.255.255.252
R3(config-if)#no shut

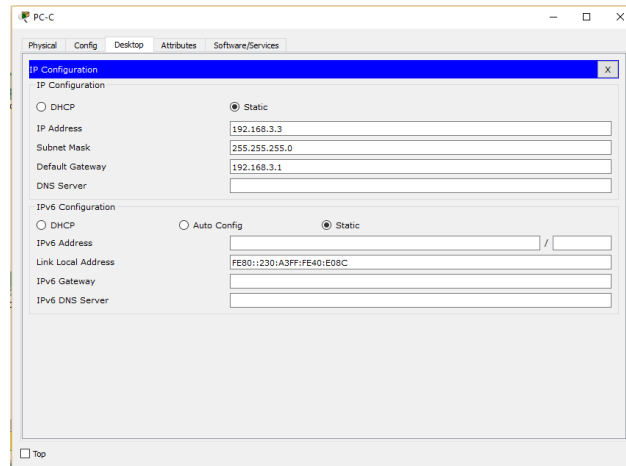
R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
```

Step 5: configurar los equipos host.



UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Step 6: Probar la conectividad.

Los routers deben poder hacerse ping entre sí, y cada computadora debe poder hacer ping a su gateway predeterminado. Las computadoras no pueden hacer ping a otras computadoras hasta que no se haya configurado el routing OSPF. Verifique y resuelva los problemas, si es necesario.

Parte 2. Configurar y verificar el enrutamiento OSPF

En la parte 2, configurará el routing OSPFv2 en todos los routers de la red y, luego, verificará que las tablas de routing se hayan actualizado correctamente. Después de verificar OSPF, configurará la autenticación de OSPF en los enlaces para mayor seguridad.

Step 7: Configure el protocolo OSPF en R1.

a. Use el comando **router ospf** en el modo de configuración global para habilitar OSPF en el R1. R1(config)# **router ospf 1**

Nota: la ID del proceso OSPF se mantiene localmente y no tiene sentido para los otros routers de la red.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



b. Configure las instrucciones **network** para las redes en el R1. Utilice la ID de área 0.

```
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
```

```
R1(config-router)# network 192.168.12.0 0.0.0.3 area 0
```

```
R1(config-router)# network 192.168.13.0 0.0.0.3 area 0
```

```
R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#network 192.168.12.0 0.0.0.3 area 0
R1(config-router)#network 192.168.13.0 0.0.0.3 area 0
R1(config-router)#
```

Step 8: Configure OSPF en el R2 y el R3.

Use el comando **router ospf** y agregue las instrucciones **network** para las redes en el R2 y el R3. Cuando el routing OSPF está configurado en el R2 y el R3, se muestran mensajes de adyacencia de vecino en el R1.

```
R1#
00:22:29: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.1 on Serial0/0/0 from
LOADING to FULL, Loading Done
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



R1#

00:23:14: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.2 on Serial0/0/1 from
LOADING to FULL, Loading Done

R1#

```
R2>en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#network 192.168.2.0 0.0.0.255 area 0
R2(config-router)#network 192.168.12.0 0.0.0.3 area 0
R2(config-router)#network 192.168.2.0 0.0.0.3 area 0
00:28:38: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.13.1 on
Serial0/0/0 from LOADING to FULL, Loading Done
R2(config-router)#network 192.168.23.0 0.0.0.3 area 0
R2(config-router)#
R2(config-router)#|
R3>en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#network 192.168.3.0 0.0.0.255 area 0
R3(config-router)#network 192.168.13.0 0.0.0.3 area 0
R3(config-router)#
-----
```

Step 9: verificar los vecinos OSPF y la información de routing.

a. Emita el comando **show ip ospf neighbor** para verificar que cada router indique a los demás routers en la red como vecinos.

R1# **show ip ospf neighbor**

```
Neighbor ID Pri State Dead Time Address Interface
192.168.23.2 0 FULL/ - 00:00:33 192.168.13.2 Serial0/0/1
192.168.23.1 0 FULL/ - 00:00:30 192.168.12.2 Serial0/0/0
```

b. Emita el comando **show ip route** para verificar que todas las redes aparezcan en la

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



tabla de routing de todos los routers.

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
O       192.168.2.0/24 [110/65] via 192.168.12.2, 00:10:01, Serial0/0/0
O       192.168.3.0/24 [110/65] via 192.168.13.2, 00:07:07, Serial0/0/1
    192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.1/32 is directly connected, Serial0/0/0
    192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/1
L       192.168.13.1/32 is directly connected, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets
--More-- |
```

R1# show ip route

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route Gateway of last resort is not set
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
O       192.168.2.0/24 [110/65] via 192.168.12.2, 00:32:33, Serial0/0/0
```


UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



- O 192.168.3.0/24 [110/65] via 192.168.13.2, 00:31:48, Serial0/0/1
192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
- C 192.168.12.0/30 is directly connected, Serial0/0/0
- L 192.168.12.1/32 is directly connected, Serial0/0/0
192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
- C 192.168.13.0/30 is directly connected, Serial0/0/1
- L 192.168.13.1/32 is directly connected, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
- O 192.168.23.0/30 [110/128] via 192.168.12.2, 00:31:38, Serial0/0/0
[110/128] via 192.168.13.2, 00:31:38, Serial0/0/1

¿Qué comando utilizaría para ver solamente las rutas OSPF en la tabla de routing?

```
R1#  
R1#show ip route ospf  
O    192.168.2.0 [110/65] via 192.168.12.2, 00:12:34, Serial0/0/0  
O    192.168.3.0 [110/65] via 192.168.13.2, 00:09:39, Serial0/0/1  
     192.168.23.0/30 is subnetted, 1 subnets  
O      192.168.23.0 [110/128] via 192.168.12.2, 00:08:45, Serial0/0/0  
                        [110/128] via 192.168.13.2, 00:08:45, Serial0/0/1  
R1#
```

Step 10: verificar la configuración del protocolo OSPF.

El comando **show ip protocols** es una manera rápida de verificar información fundamental de configuración de OSPF. Esta información incluye la ID del proceso OSPF, la ID del router, las redes que anuncia el router, los vecinos de los que el router recibe actualizaciones y la distancia administrativa predeterminada, que para OSPF es 110.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
R1#show ip protocols
```

```
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.13.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.13.1      110          00:11:03
    192.168.23.1      110          00:10:01
    192.168.23.2      110          00:10:01
  Distance: (default is 110)
```

```
R1# show ip protocols
```

```
*** IP Routing is NSF aware ***
  Routing Protocol is "ospf 1"
    Outgoing update filter list for all interfaces is not set
    Incoming update filter list for all interfaces is not set
    Router ID 192.168.13.1
    Number of areas in this router is 1. 1 normal 0 stub 0 nssa
    Maximum path: 4
    Routing for Networks:
      192.168.1.0 0.0.0.255 area 0
      192.168.12.0 0.0.0.3 area 0
      192.168.13.0 0.0.0.3 area 0
    Routing Information Sources:
      Gateway Distance Last Update
      192.168.23.2 110 00:19:16
      192.168.23.1 110 00:20:03
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Distance: (default is 110)

Step 11: verificar la información del proceso OSPF.

Use el comando **show ip ospf** para examinar la ID del proceso OSPF y la ID del router. Este comando muestra información de área OSPF y la última vez que se calculó el algoritmo SPF.

```
R1# show ip ospf
Routing Process "ospf 1" with ID 192.168.13.1
Start time: 00:20:23.260, Time elapsed: 00:25:08.296
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Supports NSSA (compatible with RFC 3101)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPF's 10000 msec
Maximum wait time between two consecutive SPF's 10000 msec
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 100 mbps
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Area BACKBONE(0)
Number of interfaces in this area is 3
Area has no authentication
SPF algorithm last executed 00:22:53.756 ago
SPF algorithm executed 7 times
Area ranges are
Number of LSA 3. Checksum Sum 0x019A61
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

```
R1#show ip ospf
```

```
Routing Process "ospf 1" with ID 192.168.13.1
```

```
Supports only single TOS(TOS0) routes  
Supports opaque LSA  
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs  
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs  
Number of external LSA 0. Checksum Sum 0x000000  
Number of opaque AS LSA 0. Checksum Sum 0x000000  
Number of DCbitless external and opaque AS LSA 0  
Number of DoNotAge external and opaque AS LSA 0  
Number of areas in this router is 1. 1 normal 0 stub 0 nssa  
External flood list length 0
```

```
Area BACKBONE(0)
```

```
Number of interfaces in this area is 3  
Area has no authentication  
SPF algorithm executed 8 times  
Area ranges are  
Number of LSA 3. Checksum Sum 0x00c59a  
Number of opaque link LSA 0. Checksum Sum 0x000000  
Number of DCbitless LSA 0  
Number of indication LSA 0  
Number of DoNotAge LSA 0  
Flood list length 0
```

Step 12: verificar la configuración de la interfaz OSPF.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



a. Emita el comando **show ip ospf interface brief** para ver un resumen de las interfaces con OSPF habilitado.

R1# **show ip ospf interface brief**

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs	F/C
Se0/0/1	1	0	192.168.13.1/30	64	P2P	1/1	
Se0/0/0	1	0	192.168.12.1/30	64	P2P	1/1	
Gi0/0	1	0	192.168.1.1/24	1	DR	0/0	

b. Para obtener una lista detallada de todas las interfaces con OSPF habilitado, emita el comando **show ip ospf interface**.

R1# **show ip ospf interface**

Serial0/0/1 is up, line protocol is up
Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement
Process ID 1, Router ID 192.168.13.1, Network Type POINT_TO_POINT, Cost: 64
Topology-MTID Cost Disabled Shutdown Topology Name
0 64 no no Base
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
Hello due in 00:00:01
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 192.168.23.2
Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
Internet Address 192.168.12.1/30, Area 0, Attached via Network Statement

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Process ID 1, Router ID 192.168.13.1, Network Type POINT_TO_POINT, Cost: 64

Topology-MTID	Cost	Disabled	Shutdown	Topology Name
0 64	no	no	Base	

Transmit Delay is 1 sec, State POINT_TO_POINT

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

oob-resync timeout 40

Hello due in 00:00:03

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 2/2, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with neighbor 192.168.23.1

Suppress hello for 0 neighbor(s)

GigabitEthernet0/0 is up, line protocol is up

Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement

Process ID 1, Router ID 192.168.13.1, Network Type BROADCAST, Cost: 1

Topology-MTID	Cost	Disabled	Shutdown	Topology Name
0 1	no	no	Base	

Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 192.168.13.1, Interface address 192.168.1.1

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

oob-resync timeout 40

Hello due in 00:00:01

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 1/1, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 0, maximum is 0

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

Step 13: Verificar la conectividad de extremo a extremo.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Se debería poder hacer ping entre todas las computadoras de la topología. Verifique y resuelva los problemas, si es necesario.

```
PC>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=2ms TTL=126
Reply from 192.168.2.3: bytes=32 time=3ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 2ms
```

```
PC>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=2ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Reply from 192.168.3.3: bytes=32 time=12ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 4ms
```

Nota: puede ser necesario desactivar el firewall de las computadoras para hacer ping entre ellas.

Parte . cambiar las asignaciones del ID del router

El ID del router OSPF se utiliza para identificar de forma única el router en el dominio de enrutamiento OSPF. Los routers Cisco derivan la ID del router en una de estas tres formas y con la siguiente prioridad:

- 1) Dirección IP configurada con el comando de OSPF **router-id**, si la hubiera
 - 2) Dirección IP más alta de cualquiera de las direcciones de loopback del router, si la hubiera
 - 3) Dirección IP activa más alta de cualquiera de las interfaces físicas del router
- Dado que no se ha configurado ningún ID o interfaz de loopback en los tres routers, el ID de router para cada ruta se determina según la dirección IP más alta de cualquier interfaz activa. En la parte 3, cambiará la asignación de ID del router OSPF con direcciones de loopback. También usará el comando **router-id** para cambiar la ID del router.

Step 1: Cambie las ID de router con direcciones de loopback.

a. Asigne una dirección IP al loopback 0 en el R1.

```
R1(config)# interface lo0
```

```
R1(config-if)# ip address 1.1.1.1 255.255.255.255
```

```
R1(config-if)# end
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
R1(config)#interface lo0

R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R1(config-if)#ip add 1.1.1.1 255.255.255.255
R1(config-if)#
```

b. Asigne direcciones IP al loopback 0 en el R2 y el R3. Utilice la dirección IP 2.2.2.2/32 para el R2 y 3.3.3.3/32 para el R3.

```
R2>en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface lo0

R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R2(config-if)#ip address 2.2.2.2 255.255.255.255
R2(config-if)#

R2>en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface lo0

R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R2(config-if)#ip address 2.2.2.2 255.255.255.255
R2(config-if)#
```

c. Guarde la configuración en ejecución en la configuración de inicio de todos los routers.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



d. Debe volver a cargar los routers para restablecer la ID del router a la dirección de loopback. Emita el comando **reload** en los tres routers. Presione Enter para confirmar

```
[OK]
R3(config)#do reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test

Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
#####|
```

e. Una vez que se haya completado el proceso de recarga del router, emita el comando **show ip protocols** para ver la nueva ID del router.

R1# **show ip protocols**

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

```
R1>en
R1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:00:52
    2.2.2.2          110          00:00:52
    3.3.3.3          110          00:02:00
  Distance: (default is 110)
```

*** IP Routing is NSF aware ***

```
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3          110          00:01:00
    2.2.2.2          110          00:01:14
  Distance: (default is 110)
```

f. Emita el comando **show ip ospf neighbor** para mostrar los cambios de ID de router de

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



los routers vecinos

```
R1#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	0	FULL/ -	00:00:37	192.168.12.2	Serial0/0/0
3.3.3.3	0	FULL/ -	00:00:31	192.168.13.2	Serial0/0/1

```
R1#
```

```
R1# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3 0		FULL/ -	00:00:35	192.168.13.2	Serial0/0/1
2.2.2.2 0		FULL/ -	00:00:32	192.168.12.2	Serial0/0/0

```
R1#
```

Step 2: cambiar la ID del router R1 con el comando router-id.

El método de preferencia para establecer la ID del router es mediante el comando **routerid**.

a. Emita el comando **router-id 11.11.11.11** en el R1 para reasignar la ID del router.

Observe el mensaje informativo que aparece al emitir el comando **router-id**.

```
R1(config)# router ospf 1
```

```
R1(config-router)# router-id 11.11.11.11
```

Reload or use "clear ip ospf process" command, for this to take effect

```
R1(config)# end
```

b. Recibirá un mensaje informativo en el que se le indique que debe volver a cargar el router o usar el comando **clear ip ospf process** para que se aplique el cambio. Emita el comando **clear ip ospf process** en los tres routers. Escriba **yes** (sí) como respuesta al mensaje de verificación de restablecimiento y presione Enter.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
R1#clear ip ospf process
Reset ALL OSPF processes? [no]: yes

R1#
00:09:24: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from FULL to DOWN,
Neighbor Down: Adjacency forced to reset

00:09:24: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from FULL to DOWN,
Neighbor Down: Interface down or detached

00:09:24: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from FULL to DOWN,
Neighbor Down: Adjacency forced to reset

00:09:24: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from FULL to DOWN,
Neighbor Down: Interface down or detached

00:09:33: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from LOADING to
FULL, Loading Done|
```

c. Establezca la ID del router R2 **22.22.22.22** y la ID del router R3 **33.33.33.33**. Luego, use el comando **clear ip ospf process** para restablecer el proceso de routing de OSPF.

d. Emita el comando **show ip protocols** para verificar que la ID del router R1 haya cambiado.

```
*** IP Routing is NSF aware ***
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 11.11.11.11
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
192.168.13.0 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/1
  Routing Information Sources:
  Gateway Distance Last Update
    33.33.33.33 110 00:00:19
    22.22.22.22 110 00:00:31
    3.3.3.3 110 00:00:41
    2.2.2.2 110 00:00:41
  Distance: (default is 110)
```

e. Emita el comando **show ip ospf neighbor** en el R1 para verificar que se muestren las nuevas ID de los routers R2 y R3.

```
R2>en
R2#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
1.1.1.1	0	FULL/ -	00:00:32	192.168.12.1	Serial0/0/0
33.33.33.33	0	FULL/ -	00:00:32	192.168.23.2	Serial0/0/1

R1# **show ip ospf neighbor**

```
Neighbor ID Pri State Dead Time Address Interface
33.33.33.33 0 FULL/ - 00:00:36 192.168.13.2 Serial0/0/1
22.22.22.22 0 FULL/ - 00:00:32 192.168.12.2 Serial0/0/0
```

Parte 2. Configurar las interfaces pasivas de OSPF

El comando **passive-interface** evita que se envíen actualizaciones de routing a través de la interfaz de router especificada. Esto se hace comúnmente para reducir el tráfico en las redes LAN, ya que no necesitan recibir comunicaciones de protocolo de routing dinámico.

En la parte 4, utilizará el comando **passive-interface** para configurar una única interfaz

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



como pasiva. También configurará OSPF para que todas las interfaces del router sean pasivas de manera predeterminada y, luego, habilitará anuncios de routing OSPF en interfaces seleccionadas.

Step 3: configurar una interfaz pasiva.

a. Emita el comando **show ip ospf interface g0/0** en el R1. Observe el temporizador que indica cuándo se espera el siguiente paquete de saludo. Los paquetes de saludo se envían cada 10 segundos y se utilizan entre los routers OSPF para verificar que sus vecinos estén activos.

```
R1# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
Topology-MTID Cost Disabled Shutdown Topology Name
  0 1 no no Base
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:02
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
```

b. Emita el comando **passive-interface** para cambiar la interfaz G0/0 en el R1 a pasiva.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



R1(config)# **router ospf 1**

R1(config-router)# **passive-interface g0/0**

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#passive-interface g0/0
R1(config-router)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

c. Vuelva a emitir el comando **show ip ospf interface g0/0** para verificar que la interfaz G0/0 ahora sea pasiva.

```
R1# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
Topology-MTID Cost Disabled Shutdown Topology Name
  0 1 no no Base
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
No Hellos (Passive interface)
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



d. Emita el comando **show ip route** en el R2 y el R3 para verificar que todavía haya disponible una ruta a la red 192.168.1.0/24.

R2# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set

```

      2.0.0.0/32 is subnetted, 1 subnets
C       2.2.2.2 is directly connected, Loopback0
O       192.168.1.0/24 [110/65] via 192.168.12.1, 00:58:32, Serial0/0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0
L       192.168.2.1/32 is directly connected, GigabitEthernet0/0
O       192.168.3.0/24 [110/65] via 192.168.23.2, 00:58:19, Serial0/0/1
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.2/32 is directly connected, Serial0/0/0
      192.168.13.0/30 is subnetted, 1 subnets
O       192.168.13.0 [110/128] via 192.168.23.2, 00:58:19, Serial0/0/1
      [110/128] via 192.168.12.1, 00:58:32, Serial0/0/0
      192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/30 is directly connected, Serial0/0/1
L       192.168.23.1/32 is directly connected, Serial0/0/1
```

Step 4: establecer la interfaz pasiva como la interfaz predeterminada en un router.

- a. Emita el comando **show ip ospf neighbor** en el R1 para verificar que el R2 aparezca como un vecino OSPF.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



R1# show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
33.33.33.33	0	FULL/ -	00:00:31	192.168.13.2	Serial0/0/1
22.22.22.22	0	FULL/ -	00:00:32	192.168.12.2	Serial0/0/0

b. Emita el comando **passive-interface default** en el R2 para establecer todas las interfaces OSPF como pasivas de manera predeterminada.

R2(config)# router ospf 1

R2(config-router)# passive-interface default

R2(config-router)#

**Apr 3 00:03:00.979: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached*

**Apr 3 00:03:00.979: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached*

c. Vuelva a emitir el comando **show ip ospf neighbor** en el R1. Una vez que el temporizador de tiempo muerto haya caducado, el R2 ya no se mostrará como un vecino OSPF.

R1#SHOW IP OSPF NEIGHBOR

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	0	FULL/ -	00:00:30	192.168.13.2	Serial0/0/1

R1#SHOW IP OSPF NEIGHBOR

R1# show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
33.33.33.33	0	FULL/ -	00:00:34	192.168.13.2	Serial0/0/1

d. Emita el comando **show ip ospf interface S0/0/0** en el R2 para ver el estado de OSPF

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



de la interfaz S0/0/0.

R2# show ip ospf interface s0/0/0

```
Serial0/0/0 is up, line protocol is up
Internet Address 192.168.12.2/30, Area 0, Attached via Network Statement
Process ID 1, Router ID 22.22.22.22, Network Type POINT_TO_POINT, Cost: 64
Topology-MTID      Cost      Disabled      Shutdown      Topology Name
  0    64         no         no             Base
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
No Hellos (Passive interface)
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
```

e. Si todas las interfaces en el R2 son pasivas, no se anuncia ninguna información de routing. En este caso, el R1 y el R3 ya no deberían tener una ruta a la red 192.168.2.0/24. Esto se puede verificar mediante el comando **show ip route**.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
R2#show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP  
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
        * - candidate default, U - per-user static route, o - ODR  
        P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
      2.0.0.0/32 is subnetted, 1 subnets  
C       2.2.2.2/32 is directly connected, Loopback0  
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks  
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0  
L       192.168.2.1/32 is directly connected, GigabitEthernet0/0  
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks  
C       192.168.12.0/30 is directly connected, Serial0/0/0  
L       192.168.12.2/32 is directly connected, Serial0/0/0  
      192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks  
C       192.168.23.0/30 is directly connected, Serial0/0/1  
L       192.168.23.1/32 is directly connected, Serial0/0/1
```

f. En el R2, emita el comando **no passive-interface** para que el router envíe y reciba actualizaciones de routing OSPF. Después de introducir este comando, verá un mensaje informativo que explica que se estableció una adyacencia de vecino con el R1.

```
R2(config)# router ospf 1
```

```
R2(config-router)# no passive-interface s0/0/0
```

```
R2(config-router)#
```

```
*Apr 3 00:18:03.463: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0  
from LOADING to FULL, Loading Done
```

g. Vuelva a emitir los comandos **show ip route** y **show ipv6 ospf neighbor** en el R1 y el R3, y busque una ruta a la red 192.168.2.0/24.

¿Qué interfaz usa el R3 para enrutarse a la red 192.168.2.0/24? [S0/0/0](#)

¿Cuál es la métrica de costo acumulado para la red 192.168.2.0/24 en el R3? [\[110/129\]](#)

¿El R2 aparece como vecino OSPF en el R1? [SI](#)

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



¿El R2 aparece como vecino OSPF en el R3? **NO**

¿Qué indica esta información?

El tráfico de la red dos 192.168.2.0/24 hacia la red tres puede ser ruteada pero a través del R1, porque la s0/0/1 en R1 está configurada como una interfaz pasiva, la información OSPF no está notificando el costo.

h. Cambie la interfaz S0/0/1 en el R2 para permitir que anuncie las rutas OSPF. Registre los comandos utilizados a continuación.

```
R2# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#no passive-interface s0/0/1
R2(config-router)#
00:49:51: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from LOADING to FULL, Loading Done
```

i. Vuelva a emitir el comando **show ip route** en el R3.

¿Qué interfaz usa el R3 para enrutarse a la red 192.168.2.0/24? **S0/0/1**

¿Cuál es la métrica de costo acumulado para la red 192.168.2.0/24 en el R3 y cómo se calcula? **65**

¿El R2 aparece como vecino OSPF del R3? **Si**

Parte 2. cambiar las métricas de OSPF

En la parte 3, cambiará las métricas de OSPF con los comandos **auto-cost**, **referencebandwidth**, **bandwidth** e **ip ospf cost**.

Nota: en la parte 1, se deberían haber configurado todas las interfaces DCE con una frecuencia de reloj de 128000.

Step 5: cambiar el ancho de banda de referencia en los routers.

El ancho de banda de referencia predeterminado para OSPF es 100 Mb/s (velocidad Fast Ethernet). Sin embargo, la mayoría de los dispositivos de infraestructura moderna

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



tienen enlaces con una velocidad superior a 100 Mb/s. Debido a que la métrica de costo de OSPF debe ser un número entero, todos los enlaces con velocidades de transmisión de 100 Mb/s o más tienen un costo de 1. Esto da como resultado interfaces Fast Ethernet, Gigabit Ethernet y 10G Ethernet con el mismo costo. Por eso, se debe cambiar el ancho de banda de referencia a un valor más alto para admitir redes con enlaces más rápidos que 100 Mb/s.

a. Emita el comando **show interface** en el R1 para ver la configuración del ancho de banda predeterminado para la interfaz G0/0.

```
R1# show interface g0/0
GigabitEthernet0/0 is up, line protocol is up
Hardware is CN Gigabit Ethernet, address is c471.fe45.7520 (bia c471.fe45.7520)
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 100 usec,
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
    Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
    ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:17:31, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
    Queueing strategy: fifo
    Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
      0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
      0 watchdog, 0 multicast, 0 pause input
    279 packets output, 89865 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
      0 unknown protocol drops
      0 babbles, 0 late collision, 0 deferred
      1 lost carrier, 0 no carrier, 0 pause output
    0 output buffer failures, 0 output buffers swapped out
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Nota: si la interfaz del equipo host solo admite velocidad Fast Ethernet, la configuración de ancho de banda de G0/0 puede diferir de la que se muestra arriba. Si la interfaz del equipo host no admite velocidad de gigabit, es probable que el ancho de banda se muestre como 100 000 Kbit/s.

b. Emita el comando **show ip route ospf** en el R1 para determinar la ruta a la red 192.168.3.0/24.

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
       + - replicated route, % - next hop override
       Gateway of last resort is not set
O 192.168.3.0/24 [110/65] via 192.168.13.2, 00:00:57, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0 [110/128] via 192.168.13.2, 00:00:57, Serial0/0/1
    [110/128] via 192.168.12.2, 00:01:08, Serial0/0/0
```

Nota: el costo acumulado del R1 a la red 192.168.3.0/24 es 65.

c. Emita el comando **show ip ospf interface** en el R3 para determinar el costo de routing para G0/0.

```
R3# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
Internet Address 192.168.3.1/24, Area 0, Attached via Network Statement
Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
Topology-MTID Cost Disabled Shutdown Topology Name
  0 1 no no Base
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.23.2, Interface address 192.168.3.1
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:05
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
  Index 1/1, flood queue length 0
    Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

d. Emita el comando **show ip ospf interface s0/0/1** en el R1 para ver el costo de routing para S0/0/1.

R1# **show ip ospf interface s0/0/1**

```
Serial0/0/1 is up, line protocol is up
Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement
Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 64
Topology-MTID    Cost    Disabled    Shutdown    Topology Name
  0    64      no         no          Base
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:04
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
  Index 3/3, flood queue length 0
    Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 192.168.23.2
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Suppress hello for 0 neighbor(s)

La suma de los costos de estas dos interfaces es el costo acumulado de la ruta a la red 192.168.3.0/24 en el R3 ($1 + 64 = 65$), como puede observarse en el resultado del comando **show ip route**.

e. Emita el comando **auto-cost reference-bandwidth 10000** en el R1 para cambiar la configuración de ancho de banda de referencia predeterminado. Con esta configuración, las interfaces de 10 Gb/s tendrán un costo de 1, las interfaces de 1 Gb/s tendrán un costo de 10, y las interfaces de 100 Mb/s tendrán un costo de 100.

```
R1(config)# router ospf 1
```

```
R1(config-router)# auto-cost reference-bandwidth 10000
```

```
% OSPF: Reference bandwidth is changed.
```

```
Please ensure reference bandwidth is consistent across all routers.
```

f. Emita el comando **auto-cost reference-bandwidth 10000** en los routers R2 y R3.

g. Vuelva a emitir el comando **show ip ospf interface** para ver el nuevo costo de G0/0 en el R3 y de S0/0/1 en el R1.

```
R3# show ip ospf interface g0/0
```

```
GigabitEthernet0/0 is up, line protocol is up  
Internet Address 192.168.3.1/24, Area 0, Attached via Network Statement  
Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 10  
Topology-MTID Cost Disabled Shutdown Topology Name  
0 10 no no Base  
Transmit Delay is 1 sec, State DR, Priority 1  
Designated Router (ID) 192.168.23.2, Interface address 192.168.3.1  
No backup designated router on this network  
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5  
oob-resync timeout 40  
Hello due in 00:00:02  
Supports Link-local Signaling (LLS)  
Cisco NSF helper support enabled  
IETF NSF helper support enabled
```


UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)

Nota: si el dispositivo conectado a la interfaz G0/0 no admite velocidad de Gigabit Ethernet, el costo será diferente del que se muestra en el resultado. Por ejemplo, el costo será de 100 para la velocidad Fast Ethernet (100 Mb/s).

10000000000/1544000 Kbit = 6476

R1# show ip ospf interface s0/0/1

Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement
Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 6476

Topology-MTID	Cost	Disabled	Shutdown	Topology Name
0 6476	no	no	Base	

Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
Hello due in 00:00:05
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 192.168.23.2
Suppress hello for 0 neighbor(s)

h. Vuelva a emitir el comando **show ip route ospf** para ver el nuevo costo acumulado de la ruta 192.168.3.0/24 (10 + 6476 = 6486).

Nota: si el dispositivo conectado a la interfaz G0/0 no admite velocidad de Gigabit Ethernet, el costo total será diferente del que se muestra en el resultado. Por ejemplo, el costo acumulado será 6576 si G0/0 está funcionando con velocidad Fast Ethernet (100 Mb/s).

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



R1# show ip route ospf

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set

```
O      192.168.2.0/24 [110/6486] via 192.168.12.2, 00:05:40, Serial0/0/0
O      192.168.3.0/24 [110/6486] via 192.168.13.2, 00:01:08, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O      192.168.23.0 [110/12952] via 192.168.13.2, 00:05:17, Serial0/0/1
      [110/12952] via 192.168.12.2, 00:05:17, Serial0/0/
```

R1#

R1#show ip route ospf

```
O      192.168.2.0 [110/6576] via 192.168.12.2, 00:18:54, Serial0/0/0
O      192.168.3.0 [110/6576] via 192.168.13.2, 00:11:29, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O      192.168.23.0 [110/12952] via 192.168.12.2, 00:11:19, Serial0/0/0
      [110/12952] via 192.168.13.2, 00:11:19, Serial0/0/1
```

R1#

Nota: cambiar el ancho de banda de referencia en los routers de 100 a 10 000 cambió los costos acumulados de todas las rutas en un factor de 100, pero el costo de cada enlace y ruta de interfaz ahora se refleja con mayor precisión.

i. Para restablecer el ancho de banda de referencia al valor predeterminado, emita el comando **auto-cost reference-bandwidth 100** en los tres routers.

R1(config)# router ospf 1

R1(config-router)# auto-cost reference-bandwidth 100

% OSPF: Reference bandwidth is changed.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Please ensure reference bandwidth is consistent across all routers.

¿Por qué querría cambiar el ancho de banda de referencia OSPF predeterminado?

Los equipos actuales soportan velocidad de enlace maroe a 100 mbits/seg, para poder obtener un costo y un calcuulo mas exacto es necesario cambiar.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#auto-cost reference-bandwidth 100
% OSPF: Reference bandwidth is changed.
    Please ensure reference bandwidth is consistent across all routers.
R1(config-router)#

R2>en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#auto-cost reference-bandwidth 100
% OSPF: Reference bandwidth is changed.
    Please ensure reference bandwidth is consistent across all routers.
R2(config-router)#

R3(config)#router ospf 1
R3(config-router)#auto-cost reference-bandwidth 100
% OSPF: Reference bandwidth is changed.
    Please ensure reference bandwidth is consistent across all routers.
R3(config-router)#
```

Step 6: cambiar el ancho de banda de una interfaz.

En la mayoría de los enlaces seriales, la métrica del ancho de banda será 1544 Kbits de manera predeterminada (la de un T1). Si esta no es la velocidad real del enlace serial, se deberá cambiar la configuración del ancho de banda para que coincida con la velocidad real, a fin de permitir que el costo de la ruta se calcule correctamente en OSPF. Use el comando **bandwidth** para ajusta la configuración del ancho de banda de una interfaz.

Nota: un concepto erróneo habitual es suponer que con el comando **bandwidth** se cambia el ancho de banda físico, o la velocidad, del enlace. El comando modifica la métrica de ancho de banda que utiliza OSPF para calcular los costos de routing, pero no modifica el ancho de banda real (la velocidad) del enlace.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



a. Emita el comando **show interface s0/0/0** en el R1 para ver la configuración actual del ancho de banda de S0/0/0. Aunque la velocidad de enlace/frecuencia de reloj en esta interfaz estaba configurada en 128 Kb/s, el ancho de banda todavía aparece como 1544 Kb/s.

R1# show interface s0/0/0

```
Serial0/0/0 is up, line protocol is up
Hardware is WIC MBRD Serial
Internet address is 192.168.12.1/30
MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
<Output Omitted>
```

b. Emita el comando **show ip route ospf** en el R1 para ver el costo acumulado de la ruta a la red 192.168.23.0/24 con S0/0/0. Observe que hay dos rutas con el mismo costo (128) a la red 192.168.23.0/24, una a través de S0/0/0 y otra a través de S0/0/1.

R1# show ip route ospf

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
+ - replicated route, % - next hop override
Gateway of last resort is not set
O 192.168.3.0/24 [110/65] via 192.168.13.2, 00:00:26, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0 [110/128] via 192.168.13.2, 00:00:26, Serial0/0/1
[110/128] via 192.168.12.2, 00:00:42, Serial0/0/0
```

c. Emita el comando **bandwidth 128** para establecer el ancho de banda en S0/0/0 en

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



128 Kb/s. R1(config)# **interface s0/0/0** R1(config-if)# **bandwidth 128**

d. Vuelva a emitir el comando **show ip route ospf**. En la tabla de routing, ya no se muestra la ruta a la red 192.168.23.0/24 a través de la interfaz S0/0/0. Esto es porque la mejor ruta, la que tiene el costo más bajo, ahora es a través de S0/0/1.

R1# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
+ - replicated route, % - next hop override
Gateway of last resort is not set
O 192.168.3.0/24 [110/65] via 192.168.13.2, 00:04:51, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0 [110/128] via 192.168.13.2, 00:04:51, Serial0/0/1

e. Emita el comando **show ip ospf interface brief**. El costo de S0/0/0 cambió de 64 a 781, que es una representación precisa del costo de la velocidad del enlace.

R1# **show ip ospf interface brief**

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs	F/C
Se0/0/1	1	0	192.168.13.1/30	64	P2P	1/1	
Se0/0/0	1	0	192.168.12.1/30	781	P2P	1/1	
Gi0/0	1	0	192.168.1.1/24	1	DR	0/0	

f. Cambie el ancho de banda de la interfaz S0/0/1 a la misma configuración que S0/0/0 en el R1

g. Vuelva a emitir el comando **show ip route ospf** para ver el costo acumulado de ambas rutas a la red 192.168.23.0/24. Observe que otra vez hay dos rutas con el mismo costo(845) a la red 192.168.23.0/24: una a través de S0/0/0 y otra a través de S0/0/1.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



R1# show ip route ospf

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
+ - replicated route, % - next hop override
Gateway of last resort is not set
O 192.168.3.0/24 [110/782] via 192.168.13.2, 00:00:09, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0 [110/845] via 192.168.13.2, 00:00:09, Serial0/0/1
[110/845] via 192.168.12.2, 00:00:09, Serial0/0/0

Explique la forma en que se calcularon los costos del R1 a las redes 192.168.3.0/24 y 192.168.23.0/30.

```
Serial0/0/1 is up, line protocol is up
Internet address is 192.168.13.1/30, Area 0
Process ID 1, Router ID 1.1.1.1, Network Type POINT-TO-POINT, Cost: 781
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:06
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 3.3.3.3
Suppress hello for 0 neighbor(s)
R1#
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



h. Emita el comando **show ip route ospf** en el R3. El costo acumulado de 192.168.1.0/24 todavía se muestra como 65. A diferencia del comando **clock rate**, el comando **bandwidth** se tiene que aplicar en ambos extremos de un enlace serial.

R3# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
+ - replicated route, % - next hop override
Gateway of last resort is not set
O 192.168.1.0/24 [110/65] via 192.168.13.1, 00:30:58, Serial0/0/0
192.168.12.0/30 is subnetted, 1 subnets
O 192.168.12.0 [110/128] via 192.168.23.1, 00:30:58, Serial0/0/1
[110/128] via 192.168.13.1, 00:30:58, Serial0/0/0

i. Emita el comando **bandwidth 128** en todas las interfaces seriales restantes de la topología.

```
R3(config)#int s0/0/0
R3(config-if)#bandwidth 128
R3(config-if)#int s0/0/1
R3(config-if)#bandwidth 128
R3(config-if)#

R2>en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int s0/0/0
R2(config-if)#bandwidth 128
R2(config-if)#int s0/0/1
R2(config-if)#bandwidth 128
R2(config-if)#
```


UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



¿Cuál es el nuevo costo acumulado a la red 192.168.23.0/24 en el R1? ¿Por qué?
1562 la suma de las dos redes

Step 7: cambiar el costo de la ruta.

De manera predeterminada, OSPF utiliza la configuración de ancho de banda para calcular el costo de un enlace. Sin embargo, puede reemplazar este cálculo si configura manualmente el costo de un enlace mediante el comando **ip ospf cost**. Al igual que el comando **bandwidth**, el comando **ip ospf cost** solo afecta el lado del enlace en el que se aplicó.

a. Emita el comando **show ip route ospf** en el R1.

R1# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
+ - replicated route, % - next hop override
Gateway of last resort is not set
O 192.168.2.0/24 [110/782] via 192.168.12.2, 00:00:26, Serial0/0/0
O 192.168.3.0/24 [110/782] via 192.168.13.2, 00:02:50, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0 [110/1562] via 192.168.13.2, 00:02:40, Serial0/0/1
[110/1562] via 192.168.12.2, 00:02:40, Serial0/0/0

b. Aplique el comando **ip ospf cost 1565** a la interfaz S0/0/1 en el R1. Un costo de 1565 es mayor que el costo acumulado de la ruta a través del R2, que es 1562.

c.

R1(config)# **int s0/0/1**

R1(config-if)# **ip ospf cost 1565**

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int s0/0/1
R1(config-if)#ip ospf cost 1565
R1(config-if)#
```

d. Vuelva a emitir el comando **show ip route ospf** en el R1 para mostrar el efecto que produjo este cambio en la tabla de routing. Todas las rutas OSPF para el R1 ahora se enrutan a través del R2.

R1# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
+ - replicated route, % - next hop override
Gateway of last resort is not set
O 192.168.2.0/24 [110/782] via 192.168.12.2, 00:02:06, Serial0/0/0
O 192.168.3.0/24 [110/1563] via 192.168.12.2, 00:05:31, Serial0/0/0
192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0 [110/1562] via 192.168.12.2, 01:14:02, Serial0/0/0

Nota: la manipulación de costos de enlace mediante el comando **ip ospf cost** es el método de preferencia y el más fácil para cambiar los costos de las rutas OSPF. Además de cambiar el costo basado en el ancho de banda, un administrador de red puede tener otros motivos para cambiar el costo de una ruta, como la preferencia por un proveedor de servicios específico o el costo monetario real de un enlace o de una ruta.

Explique la razón por la que la ruta a la red 192.168.3.0/24 en el R1 ahora atraviesa el R2.

Porque por ahí al sumar el costo de las dos rutas el costo es menos que si la tomara por la otra ruta que es 1563, si su ID es la asociado una fase multiactiva esta puede ser cambiada y por consiguiente si la interface se cae puede ocasionar cambios en el ID del

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



router, por tal motivo se debe usar una dirección loopback que no se cae o se desactiva o el comando router ID.

Reflexión

1. ¿Por qué es importante controlar la asignación de ID de router al utilizar el protocolo OSPF?

El ID de router controla el router designado alternativo en el proceso del router designado y del designado alternativo en una red de multi acceso.

2. ¿Por qué el proceso de elección de DR/BDR no es una preocupación en esta práctica de laboratorio?

Porque la elección DR/BDR no se hace en una red multiacceso como puede ser Ethernet y las seriales en este caso son de punto a punto y no se aplica el DR/BDR.

3. ¿Por qué querría configurar una interfaz OSPF como pasiva?

Al configurar la interface LAN pasiva se elimina la especificaciones de ruteo necesaria en la interface, liberando un poco de ancho de banda, el notifica a sus vecinos.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet n.º 2	Interfaz serial #1	Interfaz serial n.º 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre parentesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

Ejercicio 8.3.3.6 lab - configuring basic single-area ospfv3

Topología

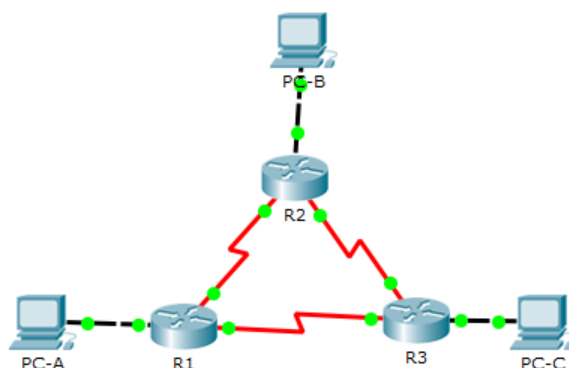


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv6	Gateway predeterminado
R1	G0/0	2001:DB8:ACAD:A::1/64 FE80::1 link-local	No aplicable
	S0/0/0 (DCE)	2001:DB8:ACAD:12::1/64 FE80::1 link-local	No aplicable
	S0/0/1	2001:DB8:ACAD:13::1/64 FE80::1 link-local	No aplicable
R2	G0/0	2001:DB8:ACAD:B::2/64 FE80::2 link-local	No aplicable
	S0/0/0	2001:DB8:ACAD:12::2/64 FE80::2 link-local	No aplicable
	S0/0/1 (DCE)	2001:DB8:ACAD:23::2/64 FE80::2 link-local	No aplicable
R3	G0/0	2001:DB8:ACAD:C::3/64 FE80::3 link-local	No aplicable
	S0/0/0 (DCE)	2001:DB8:ACAD:13::3/64 FE80::3 link-local	No aplicable
	S0/0/1	2001:DB8:ACAD:23::3/64 FE80::3 link-local	No aplicable
PC-A	NIC	2001:DB8:ACAD:A::A/64	FE80::1
PC-B	NIC	2001:DB8:ACAD:B::B/64	FE80::2
PC-C	NIC	2001:DB8:ACAD:C::C/64	FE80::3

Objetivos

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

Parte 2: configurar y verificar el routing OSPFv3

Parte 3: configurar interfaces pasivas OSPFv3

Información básica/situación

El protocolo OSPF (Open Shortest Path First) es un protocolo de routing de estado de enlace para las redes IP. Se definió OSPFv2 para redes IPv4, y OSPFv3 para redes IPv6.

En esta práctica de laboratorio, configurará la topología de la red con routing OSPFv3, asignará ID de router, configurará interfaces pasivas y utilizará varios comandos de CLI para ver y verificar la información de routing OSPFv3.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Pueden utilizarse otros routers y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios

- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



- Cables Ethernet y seriales, como se muestra en la topología

Parte 2. armar la red y configurar los parámetros básicos de los dispositivos

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos en los equipos host y los routers.

Step 8: realizar el cableado de red tal como se muestra en la topología.

Step 9: inicializar y volver a cargar los routers según sea necesario.

Step 10: configurar los parámetros básicos para cada router.

- Desactive la búsqueda del DNS.
- Configure el nombre del dispositivo como se muestra en la topología.
- Asigne **class** como la contraseña del modo EXEC privilegiado.
- Asigne **cisco** como la contraseña de vty.
- Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.
- Configure **logging synchronous** para la línea de consola.
- Cifre las contraseñas de texto no cifrado.
- Configure las direcciones link-local y de unidifusión IPv6 que se indican en la tabla de direccionamiento para todas las interfaces.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
Router(config)#hostname R1
R1(config)#int g0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shut|

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state
to up

R1(config-if)#int s0/0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:12::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#int s0/0/1
R1(config-if)#ipv6 address 2001:DB8:ACAD:13::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R1(config-if)#exit
R1(config)#ipv6 unicast-routing
R1(config)#
```

- i. Habilite el routing de unidifusión IPv6 en cada router.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#int g0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:B::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#no shut

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state
to up

R2(config-if)#int s0/0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:12::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#no shut

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R2(config-if)#int
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

^
% Invalid input detected at '^' marker.

R2(config-if)#int s0/0/1
R2(config-if)#ipv6 address 2001:DB8:ACAD:23::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#clock rate 128000
R2(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#exit
R2(config)#ipv6 unicast-routing
R2(config)#
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3
R3(config)#int g0/0
R3(config-if)#ipv6 address 2001:DB8:ACAD:C::3/64
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state
to up

R3(config-if)#int s0/0/0
R3(config-if)#ipv6 address 2001:DB8:ACAD:13::3/64
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R3(config-if)#int s0/0/1
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R3(config-if)#int s0/0/1
R3(config-if)#ipv6 address 2001:DB8:ACAD:23::3/64
R3(config-if)#ipv6 address FE80::3 link-loca
R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

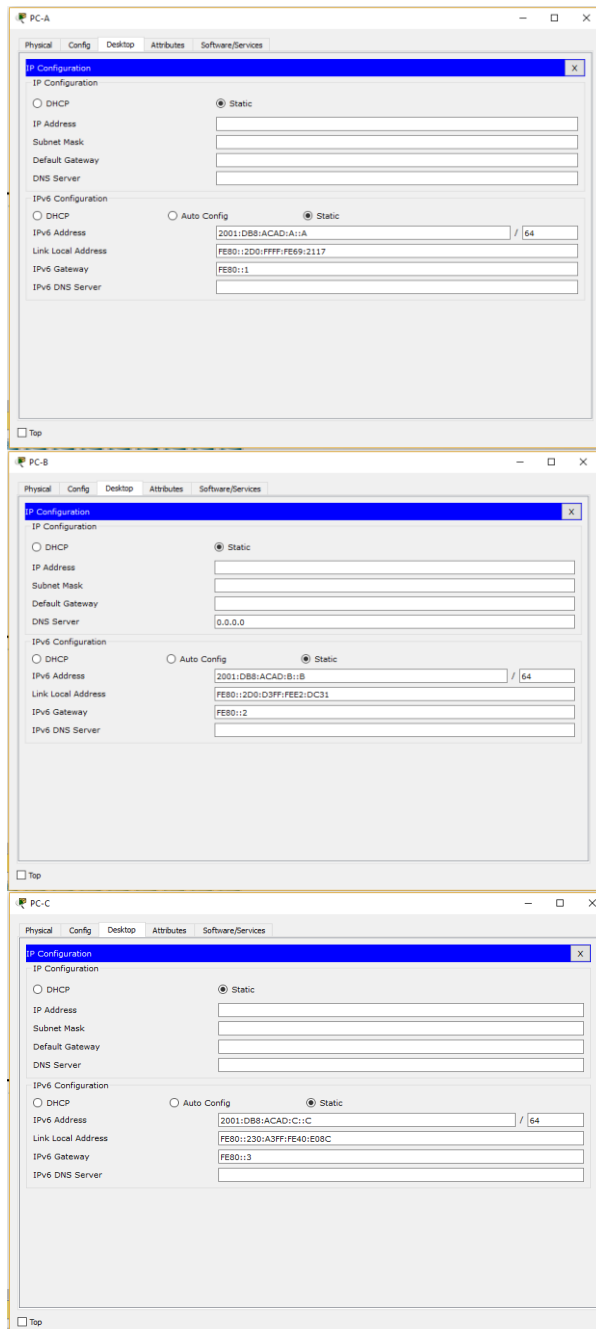
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

R3(config-if)#exit
R3(config)#ipv6 unicast-routing
R3(config)#
```

j. Copie la configuración en ejecución en la configuración de inicio

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

Step 11: configurar los equipos host.



The image displays three screenshots of the PC configuration interface for three different hosts: PC-A, PC-B, and PC-C. Each window shows the 'Config' tab with 'IP Configuration' and 'IPv6 Configuration' sections.

PC-A Configuration:

- IP Configuration:** Static IP. IP Address: [Empty], Subnet Mask: [Empty], Default Gateway: [Empty], DNS Server: [Empty].
- IPv6 Configuration:** Static. IPv6 Address: 2001:DB8:ACAD:A::A / 64, Link Local Address: FE80:12D0:FFFF:FE69:2117, IPv6 Gateway: FE80:11, IPv6 DNS Server: [Empty].

PC-B Configuration:

- IP Configuration:** Static IP. IP Address: [Empty], Subnet Mask: [Empty], Default Gateway: [Empty], DNS Server: 0.0.0.0.
- IPv6 Configuration:** Static. IPv6 Address: 2001:DB8:ACAD:B::B / 64, Link Local Address: FE80:12D0:D3FF:FE2:DC31, IPv6 Gateway: FE80:12, IPv6 DNS Server: [Empty].

PC-C Configuration:

- IP Configuration:** Static IP. IP Address: [Empty], Subnet Mask: [Empty], Default Gateway: [Empty], DNS Server: [Empty].
- IPv6 Configuration:** Static. IPv6 Address: 2001:DB8:ACAD:C::C / 64, Link Local Address: FE80:1230:A3FF:FE40:E08C, IPv6 Gateway: FE80:13, IPv6 DNS Server: [Empty].

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Step 12: Probar la conectividad.

Los routers deben poder hacerse ping entre sí, y cada computadora debe poder hacer ping a su gateway predeterminado. Las computadoras no pueden hacer ping a otras computadoras hasta que no se haya configurado el routing OSPFv3. Verifique y resuelva los problemas, si es necesario.

```
R2>en
R2#ping 2001:DB8:ACAD:B::B

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:B::B, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

R2#ping 2001:DB8:ACAD:12::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:12::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/10 ms

R2#ping 2001:DB8:ACAD:23::3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:23::3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/6 ms

---
```

Parte 2. Configurar el routing OSPFv3

En la parte 2, configurará el routing OSPFv3 en todos los routers de la red y, luego, verificará que las tablas de routing se hayan actualizado correctamente.

Step 13: asignar ID a los routers.

OSPFv3 sigue utilizando una dirección de 32 bits para la ID del router. Debido a que no hay direcciones IPv4 configuradas en los routers, asigne manualmente la ID del router

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



mediante el comando **router-id**.

a. Emita el comando **ipv6 router ospf** para iniciar un proceso OSPFv3 en el router.

```
R1(config)# ipv6 router ospf 1
```

Nota: la ID del proceso OSPF se mantiene localmente y no tiene sentido para los otros routers de la red.

b. Asigne la ID de router OSPFv3 1.1.1.1 al R1.

```
R1(config-rtr)# router-id 1.1.1.1
```

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id, please configure manually
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#
```

c. Inicie el proceso de routing de OSPFv3 y asigne la ID de router 2.2.2.2 al R2 y la ID de router 3.3.3.3 al R3.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id, please configure manually
R2(config-rtr)#router-id 2.2.2.2
R2(config-rtr)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#show ipv6 ospf
Routing Process "ospfv3 1" with ID 2.2.2.2
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps

R3>en
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ipv5 unicast-routing
^
% Invalid input detected at '^' marker.

R3(config)#ipv6 unicast-routing
R3(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id, please configure manually
R3(config-rtr)#router-id 3.3.3.3
R3(config-rtr)#
```

d. Emita el comando **show ipv6 ospf** para verificar las ID de router de todos los routers.

R2# show ipv6 ospf

```
Routing Process "ospfv3 1" with ID 2.2.2.2
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric
<Output Omitted>
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
R3#show ipv6 ospf
Routing Process "ospfv3 1" with ID 3.3.3.3
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps
```

R3#

```
R2#show ipv6 ospf
Routing Process "ospfv3 1" with ID 2.2.2.2
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps
```

R2#

```
R1#show ipv6 ospf
Routing Process "ospfv3 1" with ID 1.1.1.1
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps
```

Step 14: configurar OSPFv6 en el R1.

Con IPv6, es común tener varias direcciones IPv6 configuradas en una interfaz. La instrucción `network` se eliminó en OSPFv3. En cambio, el routing OSPFv3 se habilita en el nivel de la interfaz.

a. Emita el comando `ipv6 ospf 1 area 0` para cada interfaz en el R1 que participará en el routing OSPFv3.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
R1(config)# interface g0/0
R1(config-if)# ipv6 ospf 1 area 0
R1(config-if)# interface s0/0/0
R1(config-if)# ipv6 ospf 1 area 0
R1(config-if)# interface s0/0/1
R1(config-if)# ipv6 ospf 1 area 0
```

Nota: la ID del proceso debe coincidir con la ID del proceso que usó en el paso 1a.

b. Asigne las interfaces en el R2 y el R3 al área 0 de OSPFv3. Al agregar las interfaces al área 0, debería ver mensajes de adyacencia de vecino.

R1#

Step 15: verificar vecinos de OSPFv3.

Emita el comando **show ipv6 ospf neighbor** para verificar que el router haya formado una adyacencia con los routers vecinos. Si no se muestra la ID del router vecino o este no se muestra en el estado FULL, los dos routers no formaron una adyacencia OSPF.

R1# **show ipv6 ospf neighbor**

OSPFv3 Router with ID (1.1.1.1) (Process ID 1)

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
3.3.3.3	0	FULL/ -	00:00:39 6	Serial0/0/1	
2.2.2.2	0	FULL/ -	00:00:36 6	Serial0/0/0	

Step 16: verificar la configuración del protocolo OSPFv3.

El comando **show ipv6 protocols** es una manera rápida de verificar información fundamental de configuración de OSPFv3, incluidas la ID del proceso OSPF, la ID del router y las interfaces habilitadas para OSPFv3.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 1"
Router ID 1.1.1.1
Number of areas: 1 normal, 0 stub, 0 nssa
Interfaces (Area 0):
  Serial0/0/1
  Serial0/0/0
  GigabitEthernet0/0
  Redistrib
```

Step 17: verificar las interfaces OSPFv3.

- a. Emita el comando **show ipv6 ospf interface** para mostrar una lista detallada de cada interfaz habilitada para OSPF.

```
R1# show ipv6 ospf interface
Serial0/0/1 is up, line protocol is up
Link Local Address FE80::1, Interface ID 7
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type POINT_TO_POINT, Cost: 64
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:05
Graceful restart helper support enabled
Index 1/3/3, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 3.3.3.3
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
Link Local Address FE80::1, Interface ID 6
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```

Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:00
  Graceful restart helper support enabled
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
    Suppress hello for 0 neighbor(s)
  GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 3
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, local address FE80::1
  No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:03
  Graceful restart helper support enabled
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
    Suppress hello for 0 neighbor(s)

```

- b. Para mostrar un resumen de las interfaces con OSPFv3 habilitado, emita el comando

show ipv6 ospf interface brief.

R1# show ipv6 ospf interface brief

Interface	PID	Area	Intf ID	Cost	State	Nbrs	F/C
Se0/0/1	1	0	7	64	P2P	1/1	

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Se0/0/0	1	0	6	64	P2P	1/1
Gi0/0	1	0	3	1	DR	0/0

Step 18: verificar la tabla de routing IPv6.

Emita el comando **show ipv6 route** para verificar que todas las redes aparezcan en la tabla de routing.

R2# **show ipv6 route**

```
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001:DB8:ACAD:A::/64 [110/65]
    via FE80::1, Serial0/0/0
C   2001:DB8:ACAD:B::/64 [0/0]
    via GigabitEthernet0/0, directly connected
L   2001:DB8:ACAD:B::2/128 [0/0]
    via GigabitEthernet0/0, receive
O   2001:DB8:ACAD:C::/64 [110/65]
    via FE80::3, Serial0/0/1
C   2001:DB8:ACAD:12::/64 [0/0]
    via Serial0/0/0, directly connected
L   2001:DB8:ACAD:12::2/128 [0/0]
    via Serial0/0/0, receive
O   2001:DB8:ACAD:13::/64 [110/128]
    via FE80::3, Serial0/0/1
    via FE80::1, Serial0/0/0
C   2001:DB8:ACAD:23::/64 [0/0]
    via Serial0/0/1, directly connected
L   2001:DB8:ACAD:23::2/128 [0/0]
    via Serial0/0/1, receive
```


UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



L FF00::/8 [0/0]
via Null0, receive

```

    via Serial0/0/0, directly connected
L  2001:DB8:ACAD:12::2/128 [0/0]
    via Serial0/0/0, receive
O  2001:DB8:ACAD:13::/64 [110/128]
    via FE80::1, Serial0/0/0, receive
    via FE80::3, Serial0/0/1, receive
C  2001:DB8:ACAD:23::/64 [0/0]
    via Serial0/0/1, directly connected
L  2001:DB8:ACAD:23::2/128 [0/0]
    via Serial0/0/1, receive
L  FF00::/8 [0/0]
    via Null0, receive
R2#

```

¿Qué comando utilizaría para ver solamente las rutas OSPF en la tabla de routing?
show ipv6 route ospf

Step 19: Verificar la conectividad de extremo a extremo.

Se debería poder hacer ping entre todas las computadoras de la topología. Verifique y resuelva los problemas, si es necesario.

```

PC>ping 2001:DB8:ACAD:B::B
Pinging 2001:DB8:ACAD:B::B with 32 bytes of data:
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126

Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

PC>ping 2001:DB8:ACAD:C::C
Pinging 2001:DB8:ACAD:C::C with 32 bytes of data:
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=3ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=1ms TTL=126

Ping statistics for 2001:DB8:ACAD:C::C:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms

```

Nota: puede ser necesario desactivar el firewall de las computadoras para hacer ping entre ellas.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Parte 2. Configurar las interfaces pasivas de OSPFv3

El comando **passive-interface** evita que se envíen actualizaciones de routing a través de la interfaz de router especificada. Esto se hace comúnmente para reducir el tráfico en las redes LAN, ya que no necesitan recibir comunicaciones de protocolo de routing dinámico. En la parte 3, utilizará el comando **passive-interface** para configurar una única interfaz como pasiva. También configurará OSPFv3 para que todas las interfaces del router sean pasivas de manera predeterminada y, luego, habilitará anuncios de routing OSPF en interfaces seleccionadas.

Step 20: configurar una interfaz pasiva.

a. Emita el comando **show ipv6 ospf interface g0/0** en el R1. Observe el temporizador que indica cuándo se espera el siguiente paquete de saludo. Los paquetes de saludo se envían cada 10 segundos y se utilizan entre los routers OSPF para verificar que sus vecinos estén activos.

b.

```
R1# show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
Link Local Address FE80::1, Interface ID 3
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 1.1.1.1, local address FE80::1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:05
Graceful restart helper support enabled
Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Suppress hello for 0 neighbor(s)

- c. Emita el comando **passive-interface** para cambiar la interfaz G0/0 en el R1 a pasiva.

```
R1(config)# ipv6 router ospf 1
```

```
R1(config-rtr)# passive-interface g0/0
```

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ipv6 router ospf 1
R1(config-rtr)#passive-interface g0/0
R1(config-rtr)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

- d. Vuelva a emitir el comando **show ipv6 ospf interface g0/0** para verificar que la interfaz G0/0 ahora sea pasiva.

```
R1# show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
Link Local Address FE80::1, Interface ID 3
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State WAITING, Priority 1
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
No Hellos (Passive interface)
Wait time before Designated router selection 00:00:34
Graceful restart helper support enabled
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)

- e. Emita el comando **show ipv6 route ospf** en el R2 y el R3 para verificar que todavía haya disponible una ruta a la red 2001:DB8:ACAD:A::/64.

R2# **show ipv6 route ospf**

IPv6 Routing Table - default - 10 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2

IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external

ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect

O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

- O 2001:DB8:ACAD:A::/64 [110/65]
via FE80::1, Serial0/0/0
- O 2001:DB8:ACAD:C::/64 [110/65]
via FE80::3, Serial0/0/1
- O 2001:DB8:ACAD:13::/64 [110/128]
via FE80::3, Serial0/0/1
via FE80::1, Serial0/0/0

Step 21: establecer la interfaz pasiva como la interfaz predeterminada en el router.

- a. Emita el comando **passive-interface default** en el R2 para establecer todas las interfaces OSPFv3 como pasivas de manera predeterminada.

R2(config)# **ipv6 router ospf 1**

R2(config-rtr)# **passive-interface default**

OSPFv3 Router with ID (1.1.1.1) (Process ID 1)

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
-------------	-----	-------	-----------	--------------	-----------

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



3.3.3.3 0 FULL/ - 00:00:37 6 Serial0/0/1

c. En el R2, emita el comando **show ipv6 ospf interface s0/0/0** para ver el estado OSPF de la interfaz S0/0/0.

```
R2# show ipv6 ospf interface s0/0/0
Serial0/0/0 is up, line protocol is up
Link Local Address FE80::2, Interface ID 6
Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2
Network Type POINT_TO_POINT, Cost: 64
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
No Hellos (Passive interface)
Graceful restart helper support enabled
Index 1/2/2, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 2, maximum is 3
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
```

d. Si todas las interfaces OSPFv3 en el R2 son pasivas, no se anuncia ninguna información de routing. Si este es el caso, el R1 y el R3 ya no deberían tener una ruta a la red 2001:DB8:ACAD:B::/64. Esto se puede verificar mediante el comando **show ipv6 route**.

e. Ejecute el comando **no passive-interface** para cambiar S0/0/1 en el R2 a fin de que envíe y reciba actualizaciones de routing OSPFv3. Después de introducir este comando, aparece un mensaje informativo que explica que se estableció una adyacencia de vecino con el R3.

```
R2(config)# ipv6 router ospf 1
```

```
R2(config-rtr)# no passive-interface s0/0/1
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



- f. Vuelva a emitir los comandos **show ipv6 route** y **show ipv6 ospf neighbor** en el R1 y el R3, y busque una ruta a la red 2001:DB8:ACAD:B::/64.

¿Qué interfaz usa el R1 para enrutarse a la red 2001:DB8:ACAD:B::/64?

*2001:DB8:ACAD:B::/64 [110/129]
via FE80::3, Serial0/0/1*

¿Cuál es la métrica de costo acumulado para la red 2001:DB8:ACAD:B::/64 en el R1?
Para llegar de la red B desde R1 el costo es 129 *2001:DB8:ACAD:B::/64 [110/129]*

¿El R2 aparece como vecino OSPFv3 en el R1? *No*

¿El R2 aparece como vecino OSPFv3 en el R3? *Si*

¿Qué indica esta información?

Todo el tráfico hacia la red B desde R1, será enviada a través de R3 por la interface s0/0/0 en R2, configurada como pasiva de tal manera que OSPFv3 no envía información de ruteo a través de esta interface, el costo 129 acumulado resulta del tráfico que pasa por R3 que es el resultado de pasar por dos interfaces reales T1 de 64 Mbs y una interface LAN con costo de 1.

- g. En el R2, emita el comando **no passive-interface S0/0/0** para permitir que se anuncien las actualizaciones de routing OSPFv3 en esa interfaz.

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 router ospf 1
R2(config-rtr)#no passive-interface s0/0/0
R2(config-rtr)#
04:14:39: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done
```

- h.* Verifique que el R1 y el R2 ahora sean vecinos OSPFv3. *Si*

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



REFLEXIÓN

1. Si la configuración OSPFv6 del R1 tiene la ID de proceso 1 y la configuración OSPFv3 del R2 tiene la ID de proceso 2, ¿se puede intercambiar información de routing entre ambos routers? ¿Por qué?

R// Si, porque el proceso de SOPFv3 es solamente usado y significativamente local en un route, lo cual no necesita utilizar el proceso usado en otro router de la misma área es decir no tiene que coincidir.

2. ¿Cuál podría haber sido la razón para eliminar el comando **network** en OSPFv3?

R// Al remover la entrada network ayuda a prevenir los errores en las direcciones ipv6, una interface ipv6 puede tener múltiples direcciones asignadas a ella, asignando una interface o áreas OSPFv3 todas las redes multicas en esa interface asignadas al área OSPF y tendrán una ruta creada en la tabla de ruteo ipv6.

Tabla de resumen de interfaces del router

Resumen de interfaces del router						
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet n.º 2	Interfaz serial #1	Interfaz serial n.º 2	Interfaz serial #1	Interfaz serial n.º 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial (S0/0/0)	0/0/0	Serial (S0/0/1)	0/0/1
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial (S0/0/0)	0/0/0	Serial (S0/0/1)	0/0/1
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial (S0/1/0)	0/1/0	Serial (S0/1/1)	0/1/1
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial (S0/0/0)	0/0/0	Serial (S0/0/1)	0/0/1
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial (S0/0/0)	0/0/0	Serial (S0/0/1)	0/0/1

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

Laboratorio 9.2.1.10 Packet Tracer - Configuring Standard ACLs

Topology

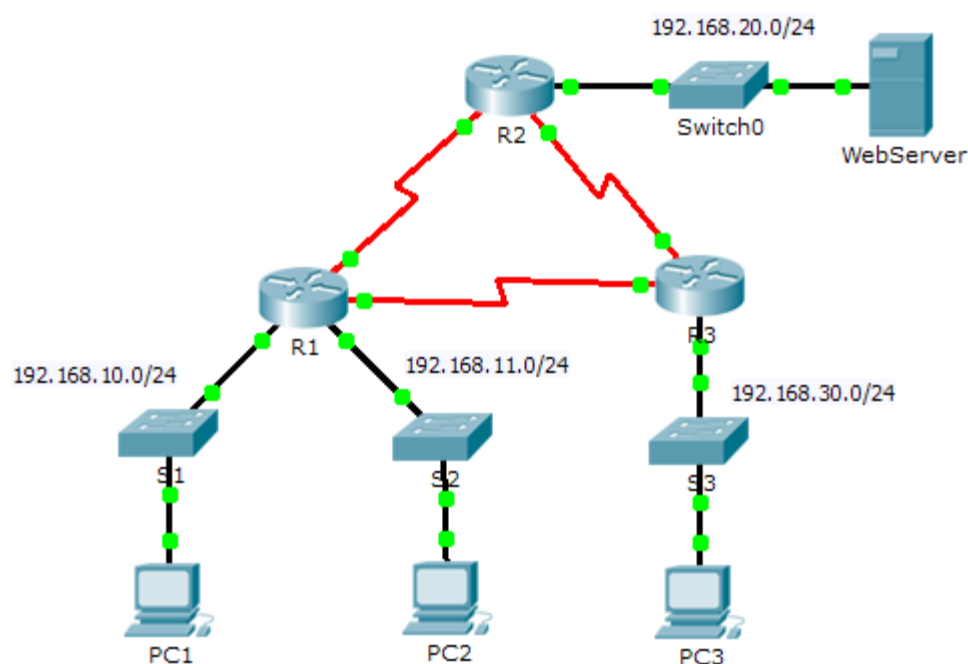


Tabla de direccionamiento

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	F0/0	192.168.10.1	255.255.255.0	N/A
	F0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.3.3.1	255.255.255.252	N/A
R2	F0/0	192.168.20.1	255.255.255.0	N/A

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



R3	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
	F0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/0	10.3.3.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
WebServer	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Objetives

Part 1: Plan an ACL Implementation

Part 2: Configure, Apply, and Verify a Standard ACL

Background / Scenario

Standard access control lists (ACLs) are router configuration scripts that control whether a router permits or denies packets based on the source address. This activity focuses on defining filtering criteria, configuring standard ACLs, applying ACLs to router interfaces, and verifying and testing the ACL implementation. The routers are already configured, including IP addresses and Enhanced Interior Gateway Routing Protocol (EIGRP) routing.

Part 1: Plan an ACL Implementation

Step 1: Investigate the current network configuration.

Before applying any ACLs to a network, it is important to confirm that you have full connectivity. Verify that the network has full connectivity by choosing a PC and pinging other devices on the network. You should be able to successfully ping every device.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Step 2: Evaluate two network policies and plan ACL implementations.

a. The following network policies are implemented on **R2**:

- The 192.168.11.0/24 network is not allowed access to the WebServer on the 192.168.20.0/24 network.
- All other access is permitted.

To restrict access from the 192.168.11.0/24 network to the WebServer at 192.168.20.254 without interfering with other traffic, an ACL must be created on **R2**. The access list must be placed on the outbound interface to the **WebServer**. A second rule must be created on **R2** to permit all other traffic.

b. The following network policies are implemented on **R3**:

- The 192.168.10.0/24 network is not allowed to communicate to the 192.168.30.0/24 network.
- All other access is permitted.

To restrict access from the 192.168.10.0/24 network to the 192.168.30.0/24 network without interfering with other traffic, an access list will need to be created on **R3**. The ACL must be placed on the outbound interface to **PC3**. A second rule must be created on **R3** to permit all other traffic.

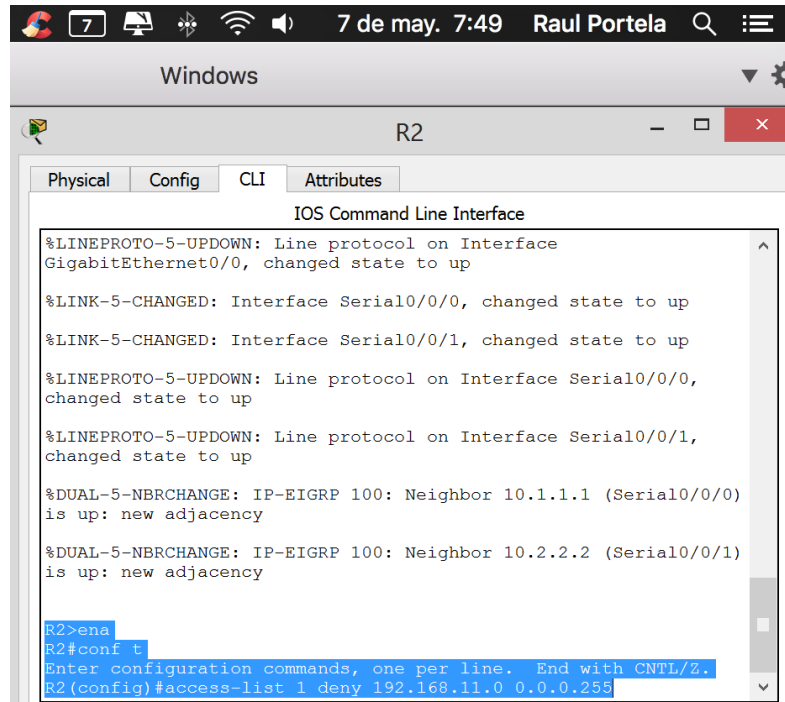
Part 2: Configure, Apply, and Verify a Standard ACL

Step 1: Configure and apply a numbered standard ACL on R2.

- #### a. Create an ACL using the number 1 on R2 with a statement that denies access to the 192.168.20.0/24 network from the 192.168.11.0/24 network.

```
R2(config)# access-list 1 deny 192.168.11.0 0.0.0.255
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

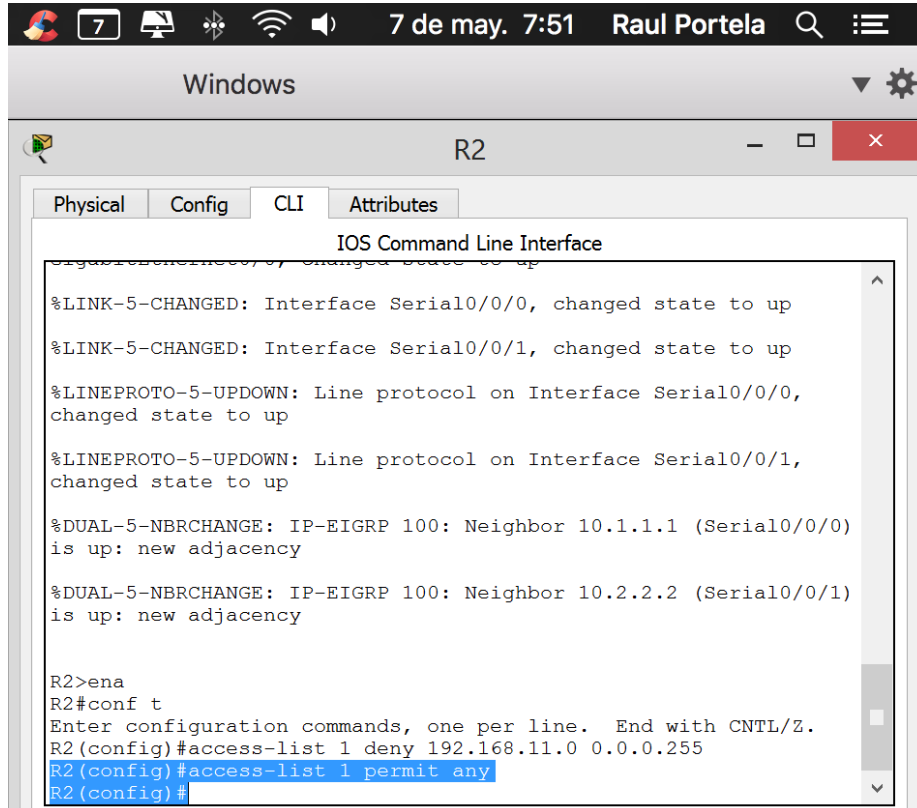


```
R2>ena
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
```

- b. By default, an access list denies all traffic that does not match a rule. To permit all other traffic, configure the following statement:

R2 (config) # **access-list 1 permit any**

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

```

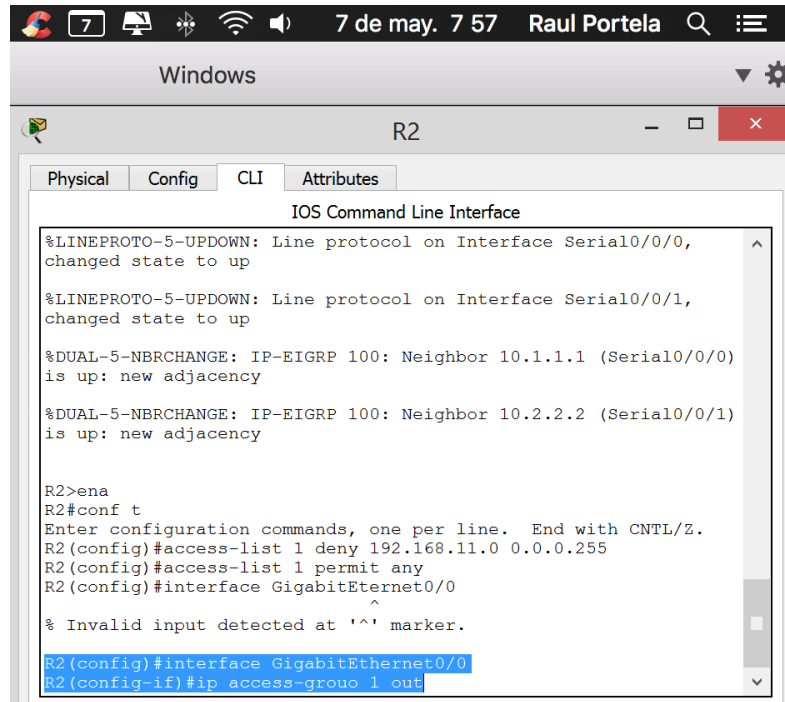
R2>ena
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#access-list 1 permit any
R2(config)#
  
```

- c. For the ACL to actually filter traffic, it must be applied to some router operation. Apply the ACL by placing it for outbound traffic on the Gigabit Ethernet 0/0 interface.

```
R2(config)# interface GigabitEthernet0/0
```

```
R2(config-if)# ip access-group 1 out
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



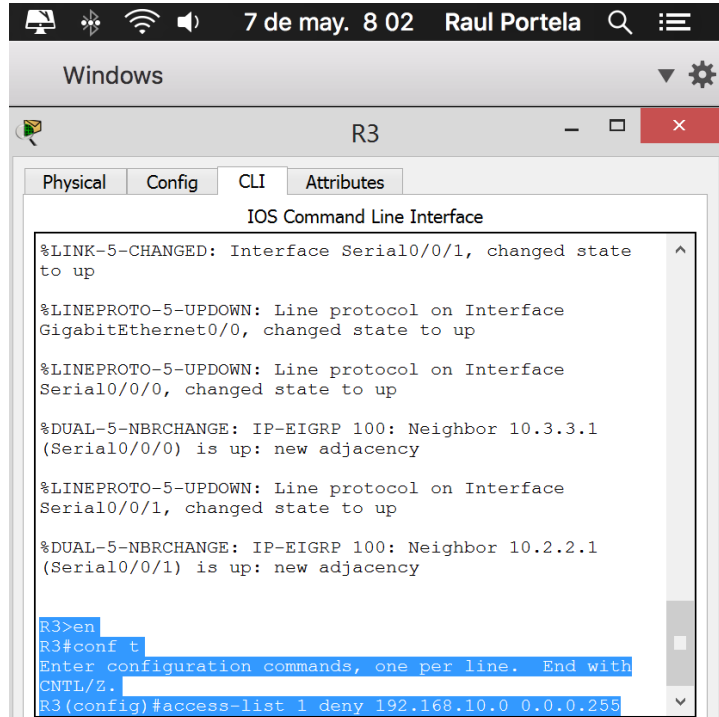
```
Windows
R2
Physical Config CLI Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.1.1.1 (Serial0/0/0)
is up: new adjacency
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.2.2.2 (Serial0/0/1)
is up: new adjacency
R2>ena
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#access-list 1 permit any
R2(config)#interface GigabitEthernet0/0
R2(config-if)#ip access-group 1 out
```

Step 2: Configure and apply a numbered standard ACL on R3.

- Create an ACL using the number 1 on **R3** with a statement that denies access to the 192.168.30.0/24 network from the PC1 (192.168.10.0/24) network.

R3(config)# **access-list 1 deny 192.168.10.0 0.0.0.255**

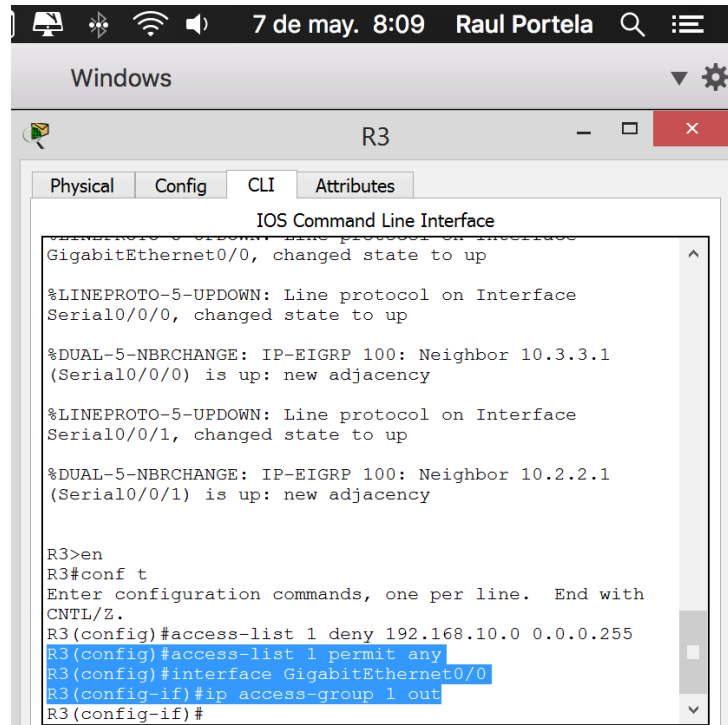
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
Windows
R3
Physical Config CLI Attributes
IOS Command Line Interface
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.3.3.1 (Serial0/0/0) is up: new adjacency
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.2.2.1 (Serial0/0/1) is up: new adjacency
R3>en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 1 deny 192.168.10.0 0.0.0.255
```

- b. By default, an ACL denies all traffic that does not match a rule. To permit all other traffic, create a second rule for ACL 1.
R3(config)# **access-list 1 permit any**
- c. Apply the ACL by placing it for outbound traffic on the Gigabit Ethernet 0/0 interface.
R3(config)# **interface GigabitEthernet0/0**
R3(config-if)# **ip access-group 1 out**

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

```

GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up

%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.3.3.1
(Serial0/0/0) is up: new adjacency

%LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up

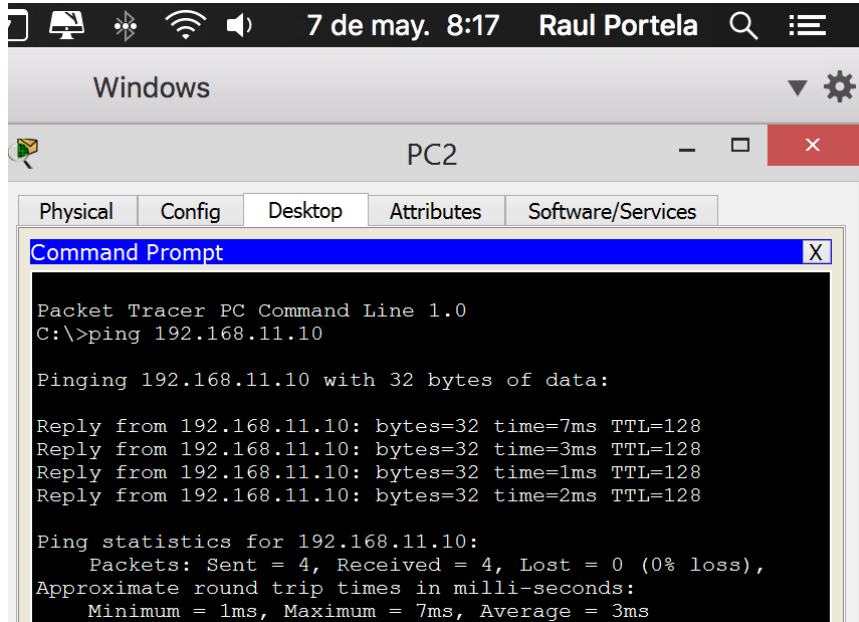
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.2.2.1
(Serial0/0/1) is up: new adjacency

R3>en
R3#conf t
Enter configuration commands, one per line. End with
CNTL/Z.
R3(config)#access-list 1 deny 192.168.10.0 0.0.0.255
R3(config)#access-list 1 permit any
R3(config)#interface GigabitEthernet0/0
R3(config-if)#ip access-group 1 out
R3(config-if)#
  
```

Step 3: Verify ACL configuration and functionality.

- On **R2** and **R3**, enter the **show access-list** command to verify the ACL configurations. Enter the **show run** or **show ip interface gigabitethernet 0/0** command to verify the ACL placements.
- With the two ACLs in place, network traffic is restricted according to the policies detailed in Part 1. Use the following tests to verify the ACL implementations:
 - A ping from 192.168.10.10 to 192.168.11.10 succeeds.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.11.10

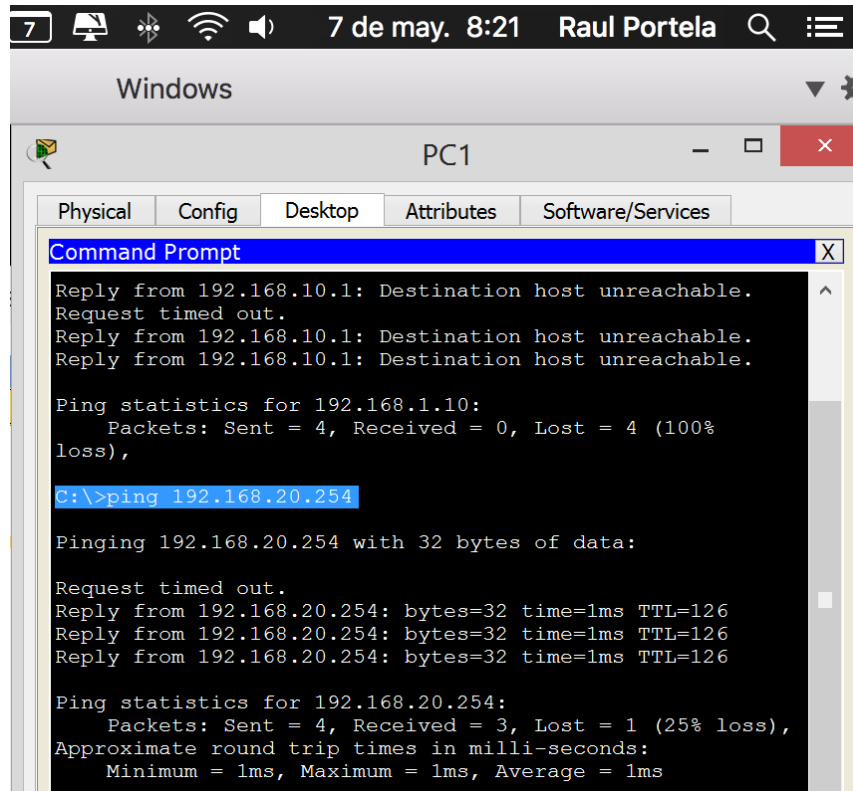
Pinging 192.168.11.10 with 32 bytes of data:

Reply from 192.168.11.10: bytes=32 time=7ms TTL=128
Reply from 192.168.11.10: bytes=32 time=3ms TTL=128
Reply from 192.168.11.10: bytes=32 time=1ms TTL=128
Reply from 192.168.11.10: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.11.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 7ms, Average = 3ms
  
```

- A ping from 192.168.10.10 to 192.168.20.254 succeeds.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```

7 7 de may. 8:21 Raul Portela
Windows
PC1
Physical Config Desktop Attributes Software/Services
Command Prompt
Reply from 192.168.10.1: Destination host unreachable.
Request timed out.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100%
loss),

C:\>ping 192.168.20.254

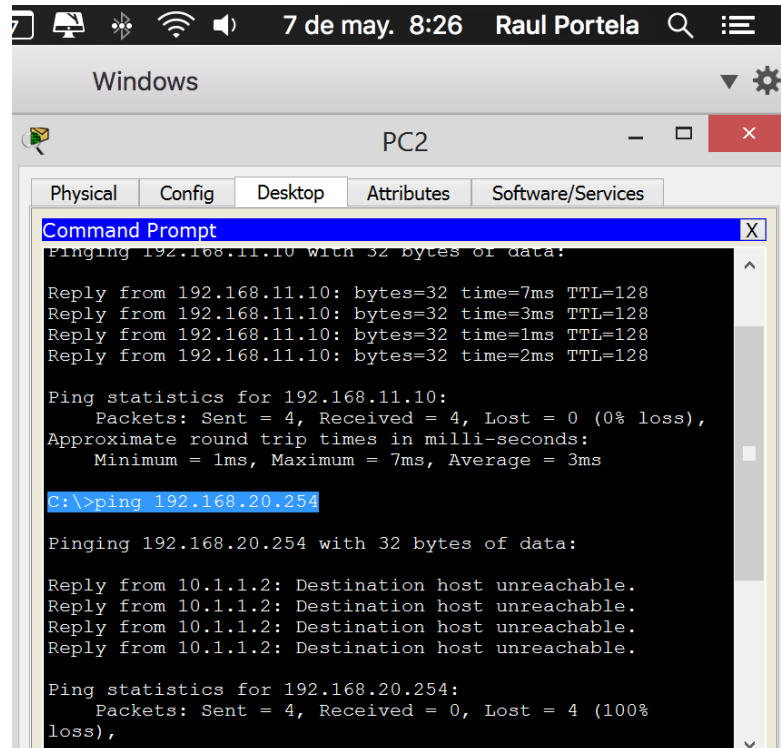
Pinging 192.168.20.254 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
  
```

- A ping from 192.168.11.10 to 192.168.20.254 fails.

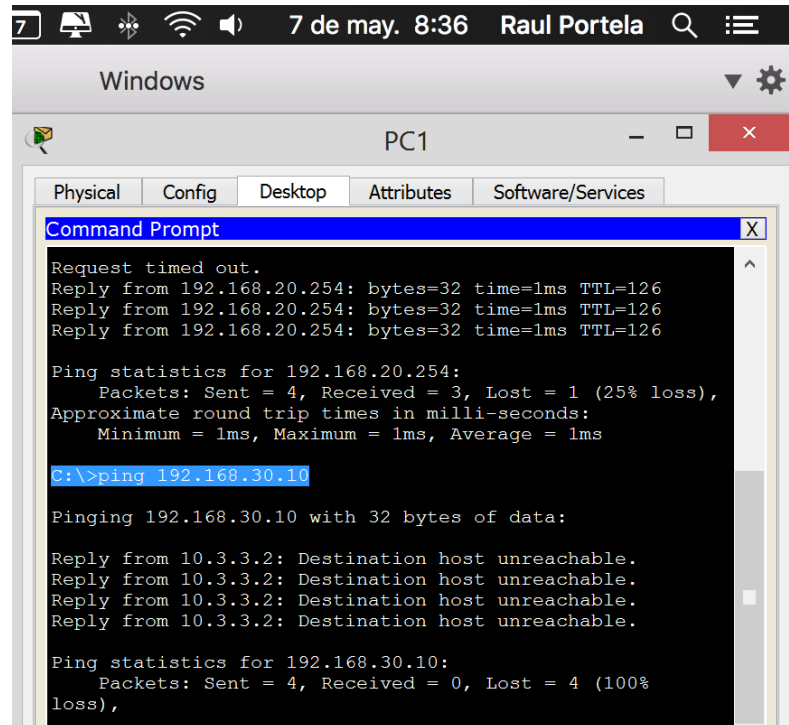
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
Windows
PC2
Physical Config Desktop Attributes Software/Services
Command Prompt
Pinging 192.168.11.10 with 32 bytes of data:
Reply from 192.168.11.10: bytes=32 time=7ms TTL=128
Reply from 192.168.11.10: bytes=32 time=3ms TTL=128
Reply from 192.168.11.10: bytes=32 time=1ms TTL=128
Reply from 192.168.11.10: bytes=32 time=2ms TTL=128
Ping statistics for 192.168.11.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 7ms, Average = 3ms
C:\>ping 192.168.20.254
Pinging 192.168.20.254 with 32 bytes of data:
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100%
loss),
```

- A ping from 192.168.10.10 to 192.168.30.10 fails.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```

Request timed out.
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ping 192.168.30.10

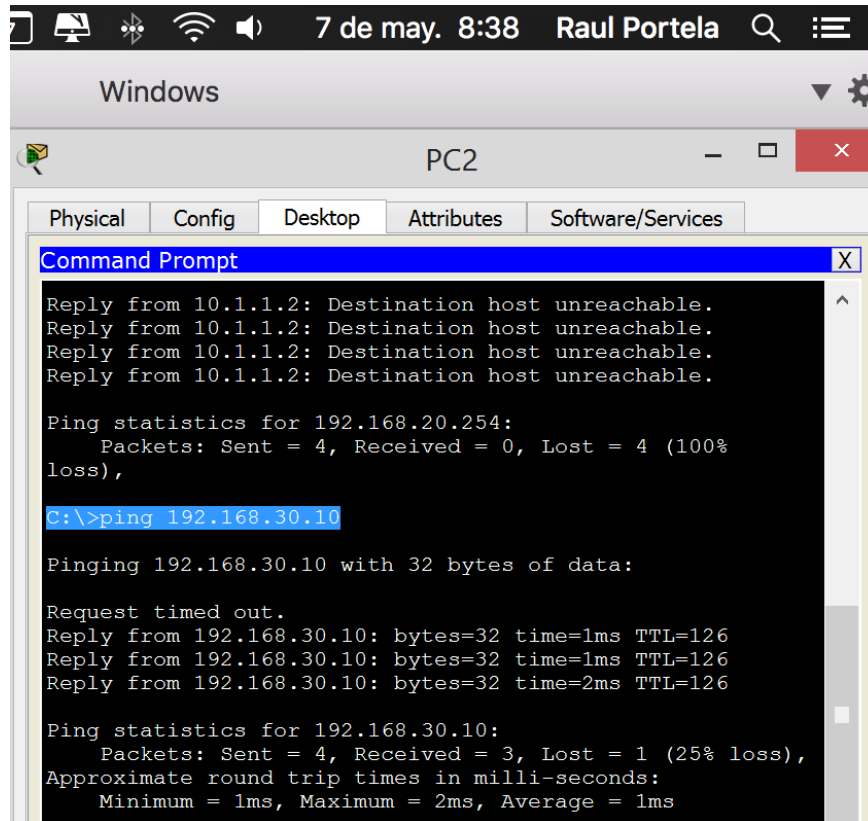
Pinging 192.168.30.10 with 32 bytes of data:

Reply from 10.3.3.2: Destination host unreachable.
Reply from 10.3.3.2: Destination host unreachable.
Reply from 10.3.3.2: Destination host unreachable.
Reply from 10.3.3.2: Destination host unreachable.

Ping statistics for 192.168.30.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100%
loss),
  
```

- A ping from 192.168.11.10 to 192.168.30.10 succeeds.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
Windows
PC2
Physical Config Desktop Attributes Software/Services
Command Prompt
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.30.10

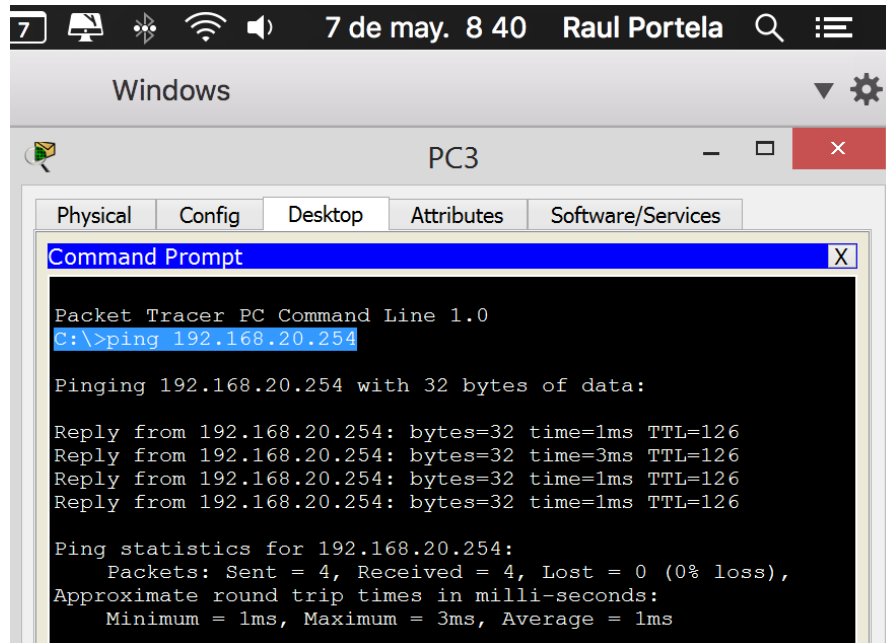
Pinging 192.168.30.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.30.10: bytes=32 time=1ms TTL=126
Reply from 192.168.30.10: bytes=32 time=1ms TTL=126
Reply from 192.168.30.10: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.30.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

- A ping from 192.168.30.10 to 192.168.20.254 succeeds.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=3ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms
```

Activity Results

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Windows

Cisco Packet Tracer - \\Mac\Home\Documents\Ing Electronica\DIPLMADO DE PR...

File Edit Options View Tools Extensions Help

Activity Results Time Elapsed: 19:57:45

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Points	Compon	Feed
Network				
R2				
ACL		0	ACL	
✓ 1	Correct	25	IPv4 S...	
Ports		0	Other	
GigabitEthernet0/0		0	Other	
✓ Access-group...	Correct	25	IPv4 S...	
R3				
ACL		0	ACL	
✓ 1	Correct	25	IPv4 S...	
Ports		0	Other	
GigabitEthernet0/0		0	Other	
✓ Access-group...	Correct	25	IPv4 S...	

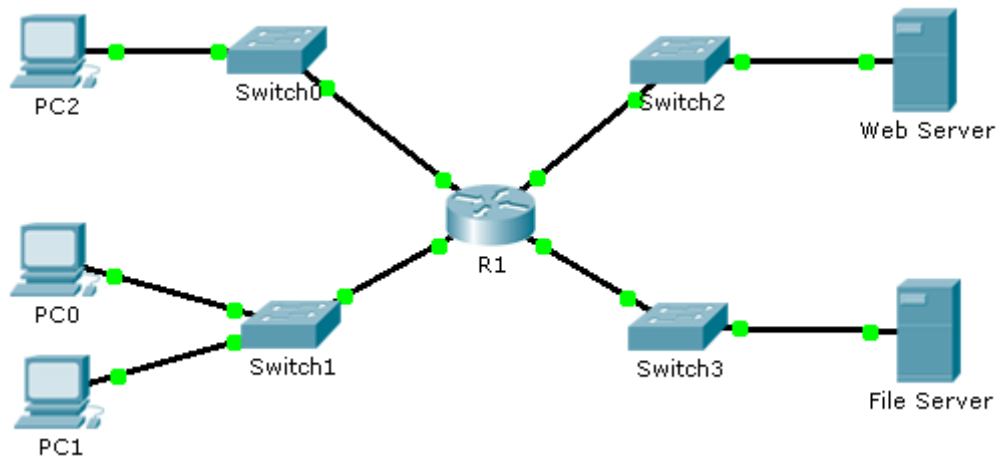
Component	Items/Total	Score
IPv4 Standard ACL Implementation	4/4	100/100

Score : 100/100
Item Count : 4/4

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
 Escuela de ciencias básicas tecnologías e Ingeniería
 DIPLOMADO DE PROFUNDIZACION CISCO
 2017 I

Laboratorio 9.2.1.11 Packet Tracer - Configuring Named Standard ACLs

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	F0/0	192.168.10.1	255.255.255.0	N/A
	F0/1	192.168.20.1	255.255.255.0	N/A
	E0/0/0	192.168.100.1	255.255.255.0	N/A
	E0/1/0	192.168.200.1	255.255.255.0	N/A
File Server	NIC	192.168.200.100	255.255.255.0	192.168.200.1
Web Server	NIC	192.168.100.100	255.255.255.0	192.168.100.1
PC0	NIC	192.168.20.3	255.255.255.0	192.168.20.1
PC1	NIC	192.168.20.4	255.255.255.0	192.168.20.1

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



PC2	NIC	192.168.10.3	255.255.255.0	192.168.10.1
-----	-----	--------------	---------------	--------------

Objectives

Part 1: Configure and Apply a Named Standard ACL

Part 2: Verify the ACL Implementation

Background / Scenario

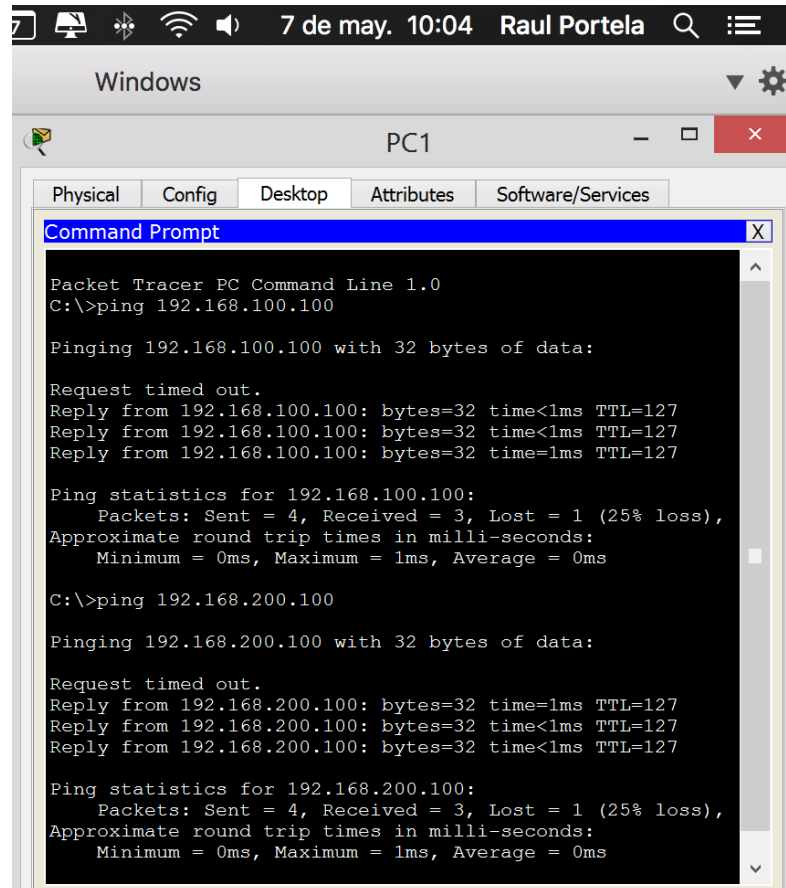
The senior network administrator has tasked you to create a standard named ACL to prevent access to a file server. All clients from one network and one specific workstation from a different network should be denied access.

Part 1: Configure and Apply a Named Standard ACL

Step 1: Verify connectivity before the ACL is configured and applied.

All three workstations should be able to ping both the **Web Server** and **File Server**.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



The screenshot shows a Windows desktop environment. At the top, a taskbar displays the date and time as '7 de may. 10:04' and the user name 'Raul Portela'. Below the taskbar, a window titled 'PC1' is open, showing the 'Desktop' tab. A 'Command Prompt' window is active, displaying the output of two ping commands. The first command is 'ping 192.168.100.100', which shows a 'Request timed out.' followed by three successful replies from 192.168.100.100. The second command is 'ping 192.168.200.100', which also shows a 'Request timed out.' followed by three successful replies from 192.168.200.100. Both ping statistics show 4 packets sent, 3 received, and 1 lost (25% loss).

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.200.100: bytes=32 time=1ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Step 2: Configure a named standard ACL.

Configure the following named ACL on R1.

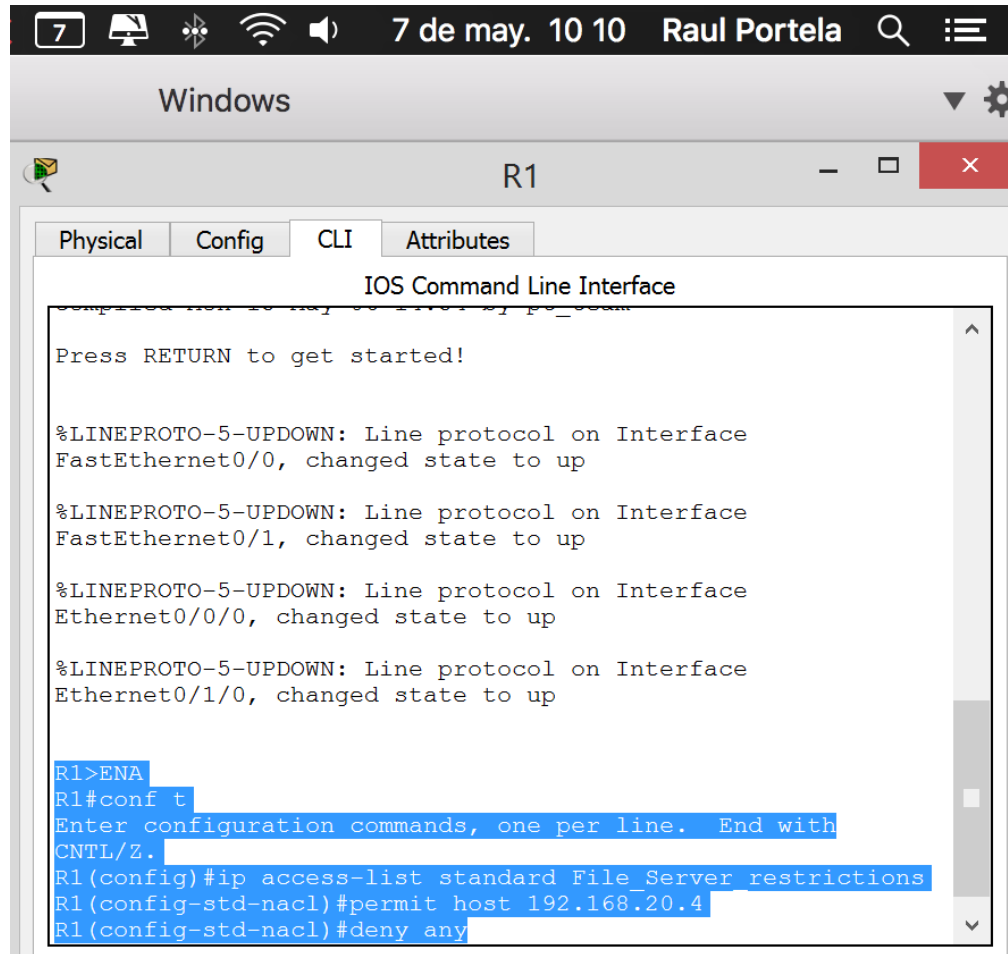
```
R1(config)# ip access-list standard File_Server_Restrictions
```

```
R1(config-std-nacl)# permit host 192.168.20.4
```

```
R1(config-std-nacl)# deny any
```

Note: For scoring purposes, the ACL name is case-sensitive.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```

Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet0/0/0, changed state to up

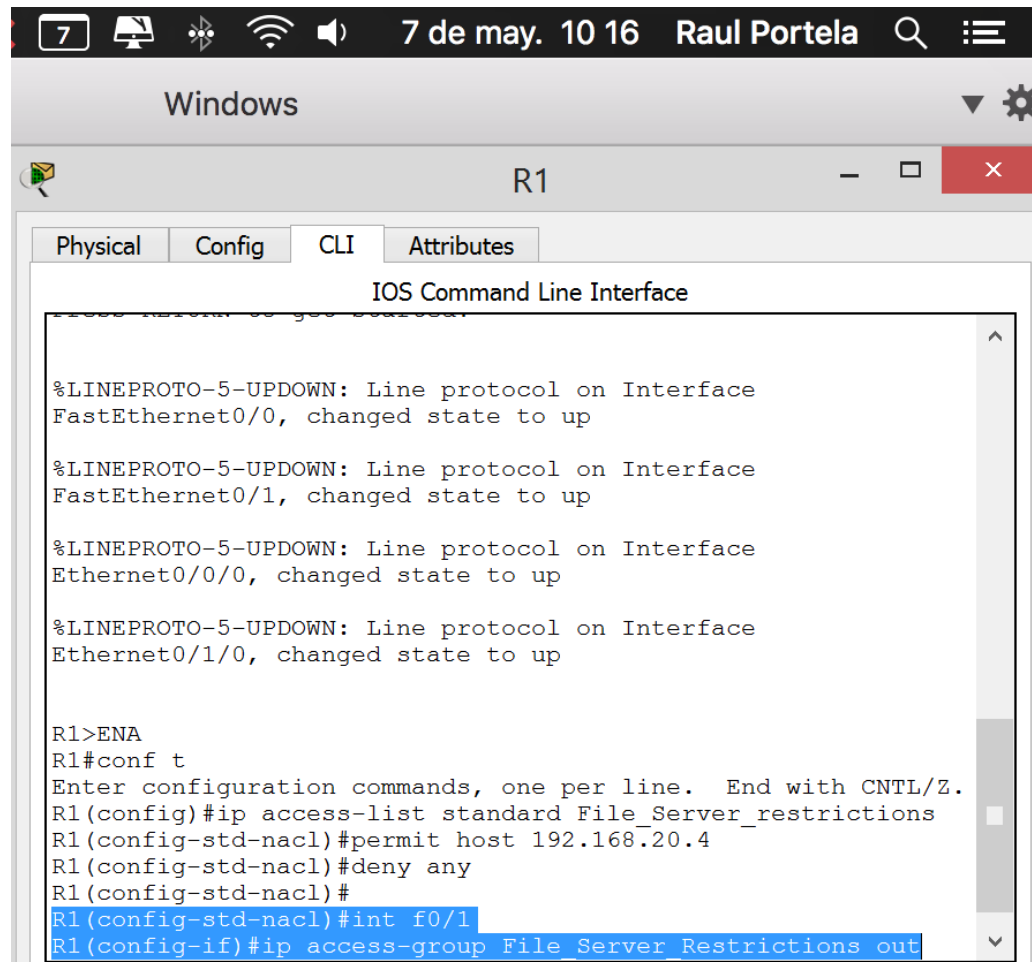
%LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet0/1/0, changed state to up

R1>ENA
R1#conf t
Enter configuration commands, one per line. End with
CNTL/Z.
R1(config)#ip access-list standard File_Server restrictions
R1(config-std-nacl)#permit host 192.168.20.4
R1(config-std-nacl)#deny any
  
```

Step 3: Apply the named ACL.

- Apply the ACL outbound on the interface Fast Ethernet 0/1.
R1(config-if) # **ip access-group File_Server_Restrictions out**
- Save the configuration.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
R1
Physical Config CLI Attributes
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet0/1/0, changed state to up

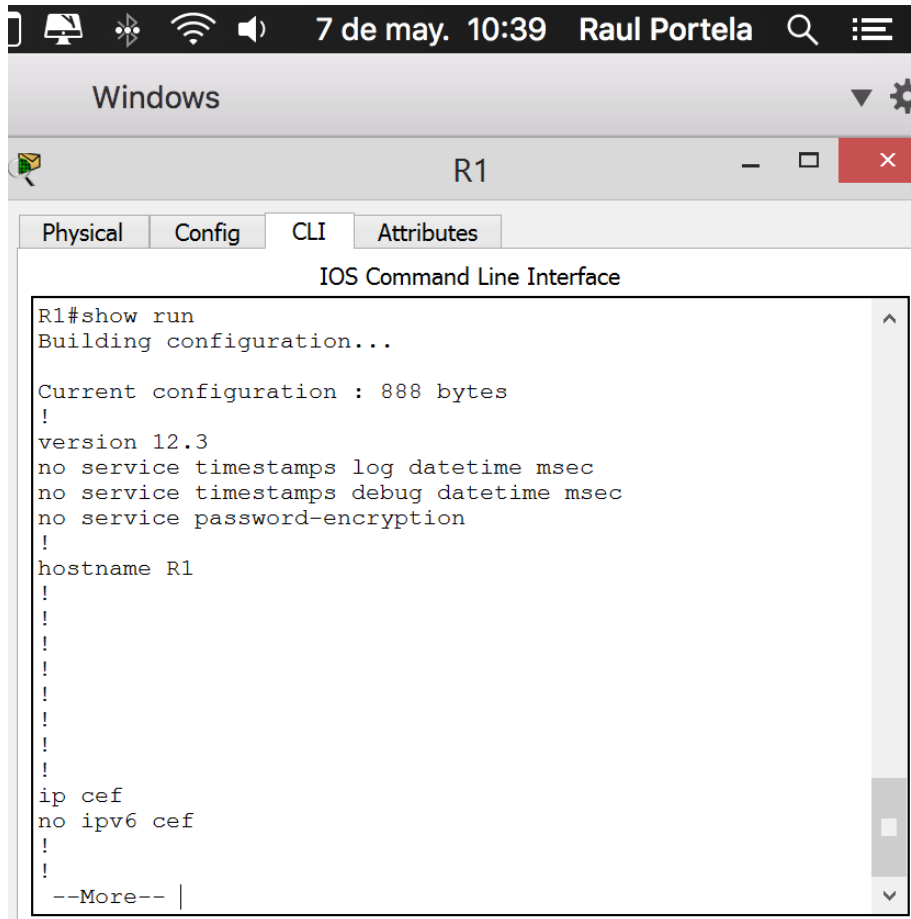
R1>ENA
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip access-list standard File_Server_restrictions
R1(config-std-nacl)#permit host 192.168.20.4
R1(config-std-nacl)#deny any
R1(config-std-nacl)#
R1(config-std-nacl)#int f0/1
R1(config-if)#ip access-group File_Server_Restrictions out
```

Part 2: Verify the ACL Implementation

Step 1: Verify the ACL configuration and application to the interface.

Use the **show access-lists** command to verify the ACL configuration. Use the **show run** or **show ip interface fastethernet 0/1** command to verify that the ACL is applied correctly to the interface.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



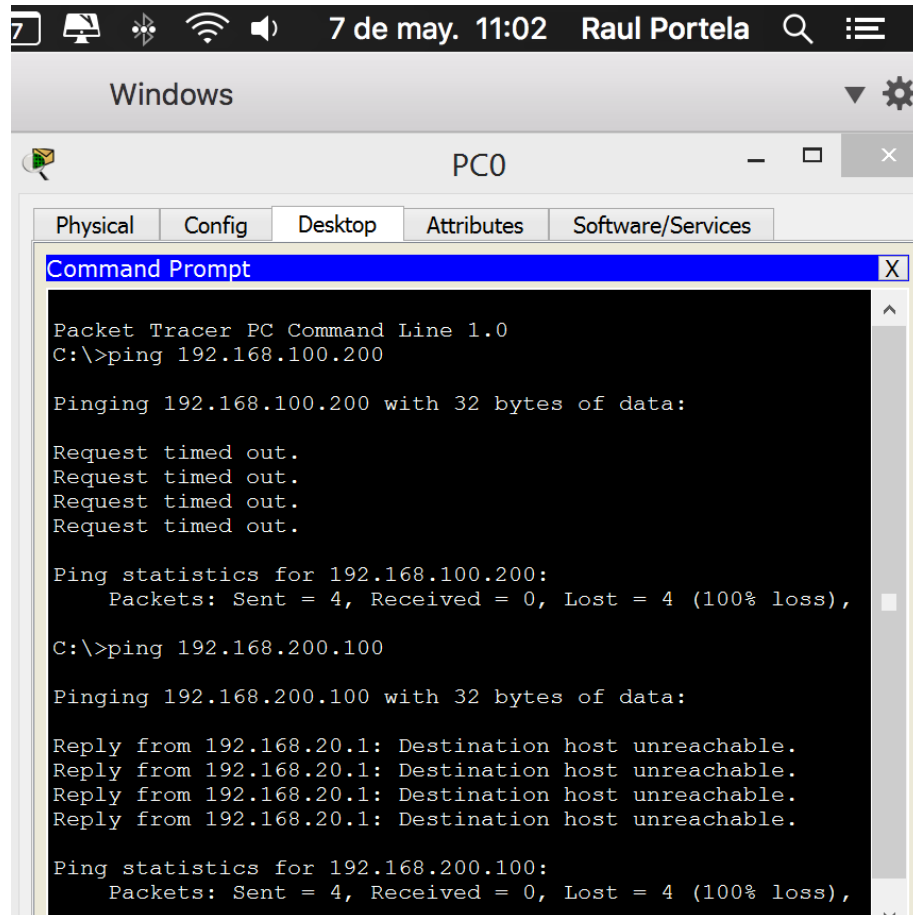
```
R1#show run
Building configuration...

Current configuration : 888 bytes
!
version 12.3
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
--More-- |
```

Step 2: Verify that the ACL is working properly.

All three workstations should be able to ping the **Web Server**, but only **PC1** should be able to ping the **File Server**.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



The screenshot shows a Windows-style interface for a PC named 'PC0'. The 'Desktop' tab is selected, displaying a 'Command Prompt' window. The command prompt shows the results of two ping commands. The first command, 'ping 192.168.100.200', results in four 'Request timed out.' messages and a 100% loss of packets. The second command, 'ping 192.168.200.100', results in four 'Destination host unreachable.' messages and a 100% loss of packets.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.100.200

Pinging 192.168.100.200 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.100.200:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

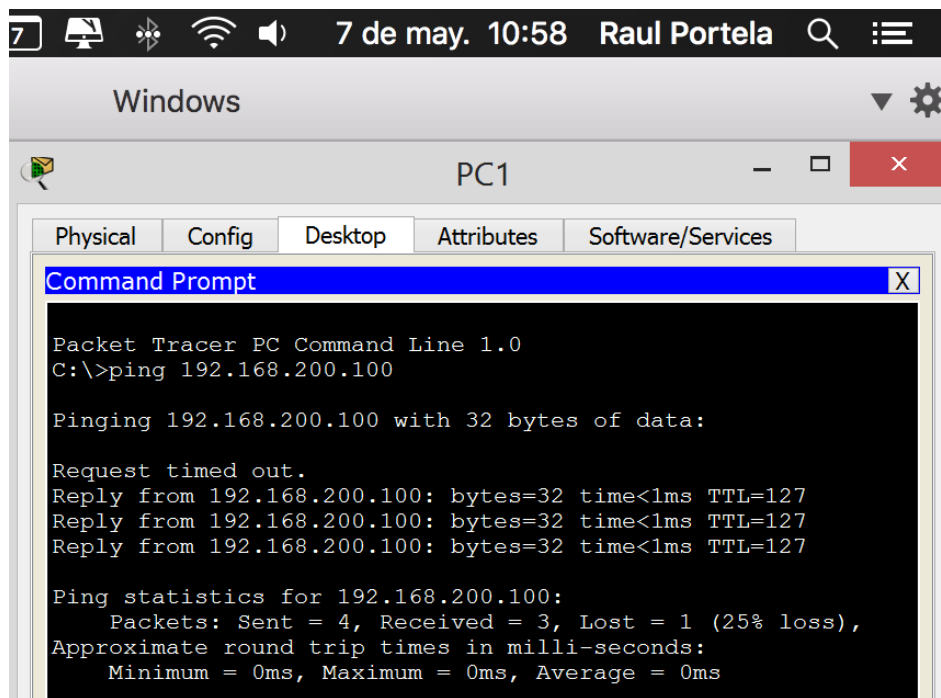
C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



The screenshot shows a Windows-style interface for a Packet Tracer PC named 'PC1'. The 'Desktop' tab is selected, displaying a 'Command Prompt' window. The command prompt shows the execution of the command 'C:\>ping 192.168.200.100'. The output indicates that the first ping request timed out, while the subsequent three succeeded with 32 bytes of data, a time of less than 1ms, and a TTL of 127. The final statistics show 4 packets sent, 3 received, and 1 lost (25% loss), with all round trip times being 0ms.

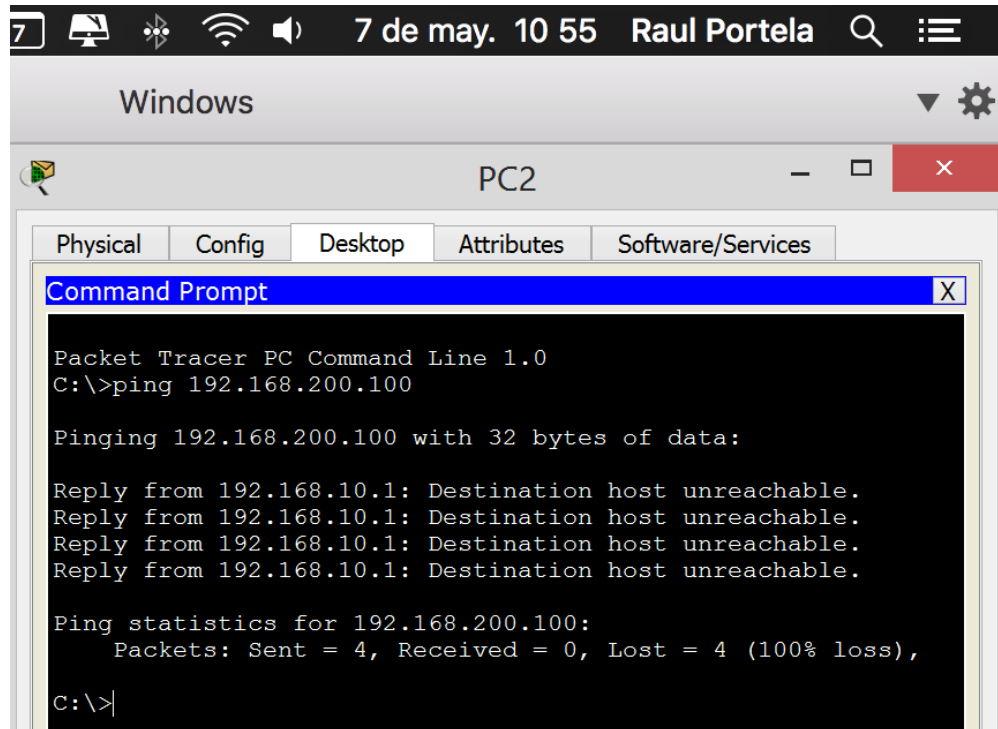
```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



The screenshot shows a Windows-style interface for a PC named 'PC2'. The 'Desktop' tab is selected, displaying a 'Command Prompt' window. The command prompt shows the execution of a ping command to 192.168.200.100, which fails with 100% loss. The output text is as follows:

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

Activity Results

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
 Escuela de ciencias básicas tecnologías e Ingeniería
 DIPLOMADO DE PROFUNDIZACION CISCO
 2017 I



100% 7 de may. 11 08 Raul Portela

Windows

Cisco Packet Tracer - \\Mac\Home\Documents\Ing Electronica\DIPLMADO DE ...

File Edit Options View Tools Extensions Help

Activity Results Time Elapsed: 00:23:52

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Poir	Component
Network			
R1			
ACL		0	ACL
✓ File_Server_Restri...	Correct	80	IPv4 Stand
Ports		0	Other
FastEthernet0/1		0	Other
✓ Access-group Out	Correct	20	IPv4 Stand

Component	Items/Total	Score
IPv4 Standard ACL Implementation	2/2	100/100

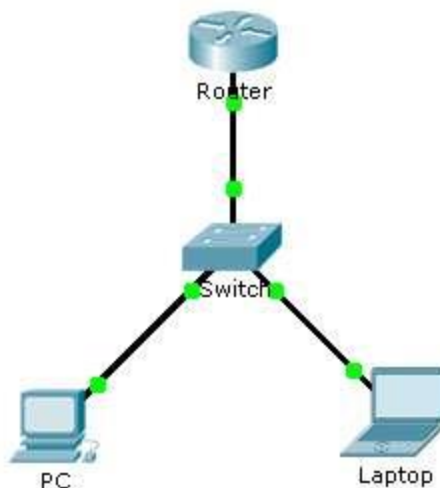
Close

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Laboratorio 9.2.3.3 Packet Tracer - Configuring an ACL on VTY Lines

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Router	F0/0	10.0.0.254	255.0.0.0	N/A
PC	NIC	10.0.0.1	255.0.0.0	10.0.0.254
Laptop	NIC	10.0.0.2	255.0.0.0	10.0.0.254

Objectives

Part 1: Configure and Apply an ACL to VTY Lines

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Part 2: Verify the ACL Implementation

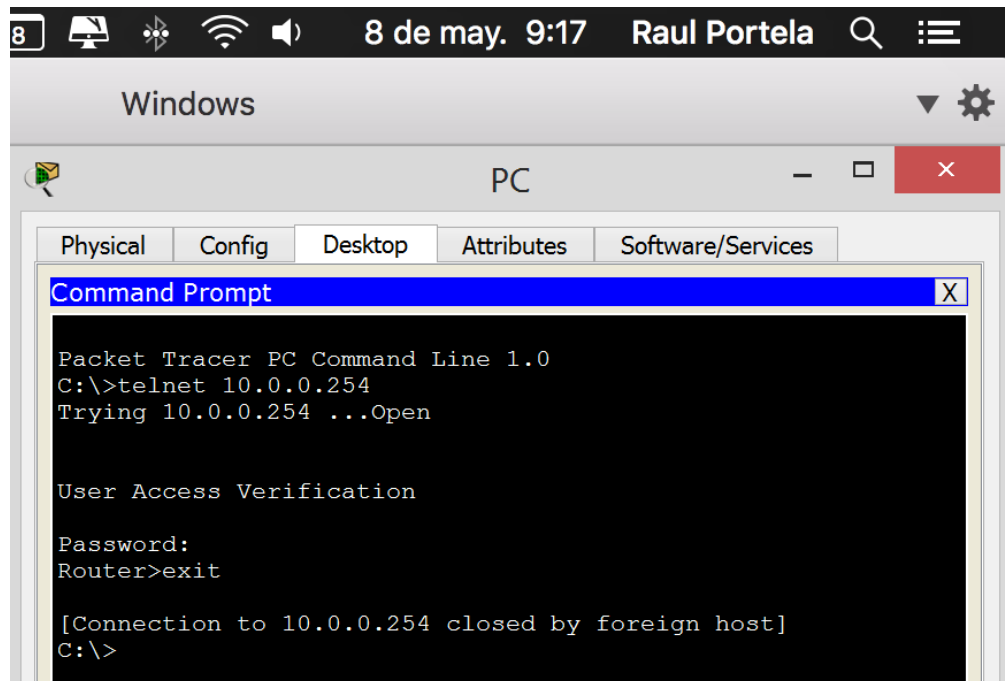
Background

As network administrator, you must have remote access to your router. This access should not be available to other users of the network. Therefore, you will configure and apply an access control list (ACL) that allows **PC** access to the Telnet lines, but denies all other source IP addresses.

Part 1: Configure and Apply an ACL to VTY Lines

Step 1: Verify Telnet access before the ACL is configured.

Both computers should be able to Telnet to the **Router**. The password is **cisco**.



```
Packet Tracer PC Command Line 1.0
C:\>telnet 10.0.0.254
Trying 10.0.0.254 ...Open

User Access Verification

Password:
Router>exit

[Connection to 10.0.0.254 closed by foreign host]
C:\>
```

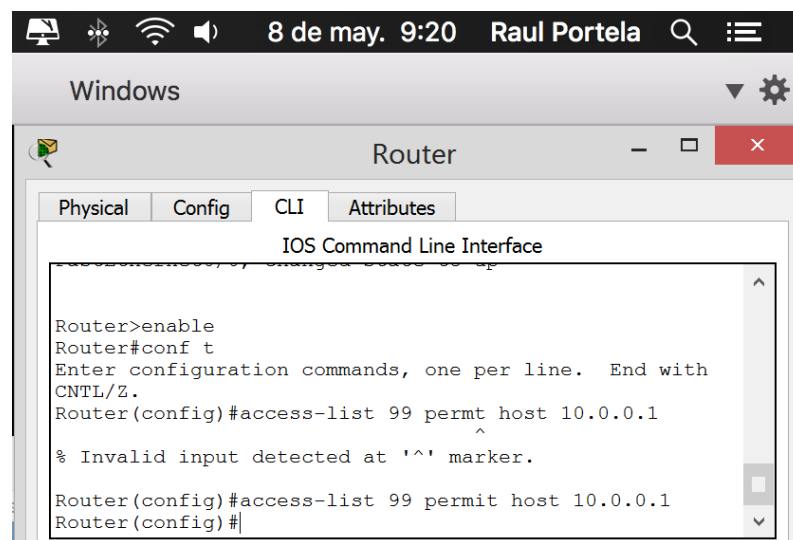
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Step 2: Configure a numbered standard ACL.

Configure the following numbered ACL on **Router**.

```
Router(config)# access-list 99 permit host 10.0.0.1
```



Because we do not want to permit access from any other computers, the implicit deny property of the access list satisfies our requirements.

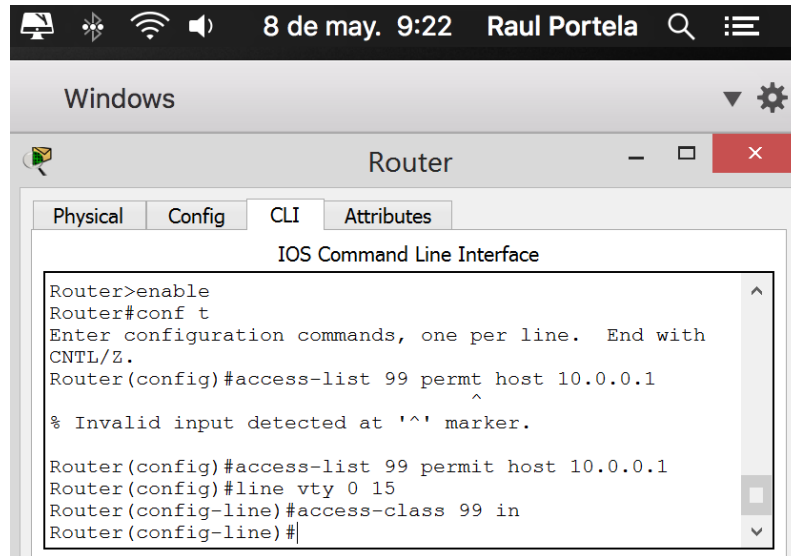
Step 3: Place a named standard ACL on the router.

Access to the **Router** interfaces must be allowed, while Telnet access must be restricted. Therefore, we must place the ACL on Telnet lines 0 through 4. From the configuration prompt of **Router**, enter line configuration mode for lines 0 – 4 and use the **access-class** command to apply the ACL to all the VTY lines:

```
Router(config)# line vty 0 15
```

```
Router(config-line)# access-class 99 in
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#access-list 99 permt host 10.0.0.1
                                     ^
% Invalid input detected at '^' marker.

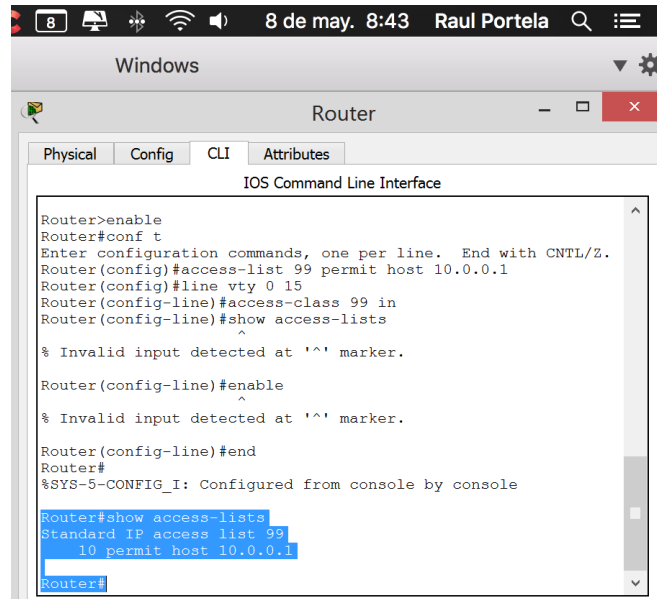
Router(config)#access-list 99 permit host 10.0.0.1
Router(config)#line vty 0 15
Router(config-line)#access-class 99 in
Router(config-line)#
```

Part 2: Verify the ACL Implementation

Step 1: Verify the ACL configuration and application to the VTY lines.

Use the **show access-lists** to verify the ACL configuration. Use the **show run** command to verify the ACL is applied to the VTY lines.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 99 permit host 10.0.0.1
Router(config)#line vty 0 15
Router(config-line)#access-class 99 in
Router(config-line)#show access-lists

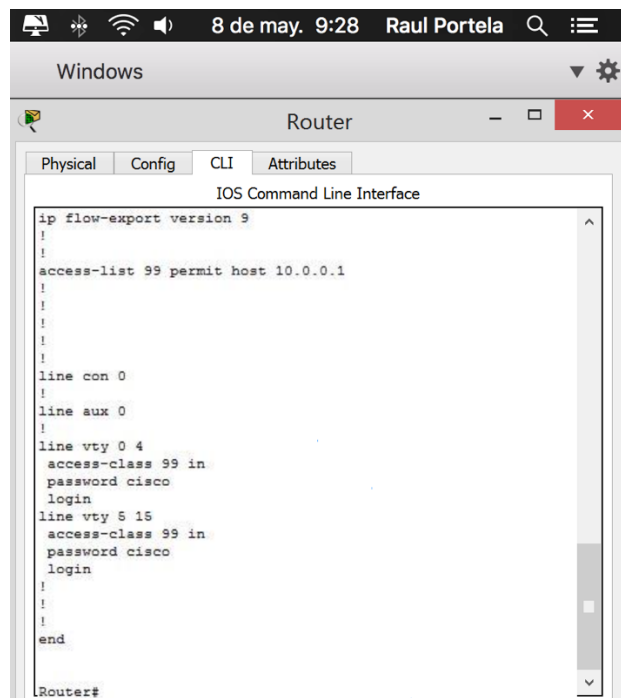
% Invalid input detected at '^' marker.

Router(config-line)#enable

% Invalid input detected at '^' marker.

Router(config-line)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show access-lists
Standard IP access list 99
 10 permit host 10.0.0.1
Router#
```



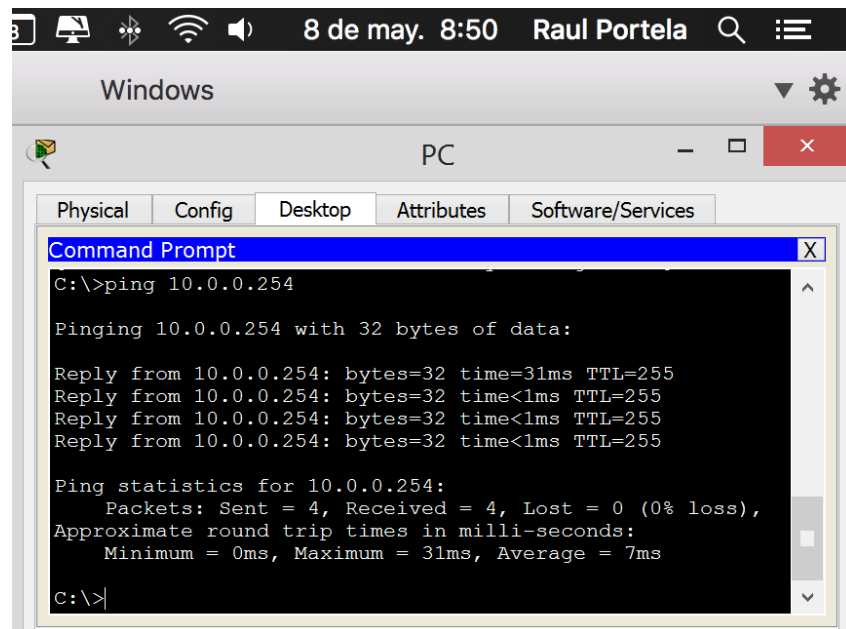
```
ip flow-export version 9
!
!
access-list 99 permit host 10.0.0.1
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 access-class 99 in
 password cisco
 login
line vty 5 15
 access-class 99 in
 password cisco
 login
!
!
!
end
Router#
```

Step 2: Verify that the ACL is working properly.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Both computers should be able to ping the **Router**, but only **PC** should be able to Telnet to it.



The screenshot shows a Windows desktop environment. At the top, the taskbar displays system icons (network, volume, battery), the date and time '8 de may. 8:50', and the user name 'Raul Portela'. A window titled 'Windows' is open, showing a 'PC' icon. Below it, a 'Command Prompt' window is active, displaying the results of a ping command to 10.0.0.254. The output shows four successful replies with 0% loss and a 7ms average round trip time.

```
C:\>ping 10.0.0.254

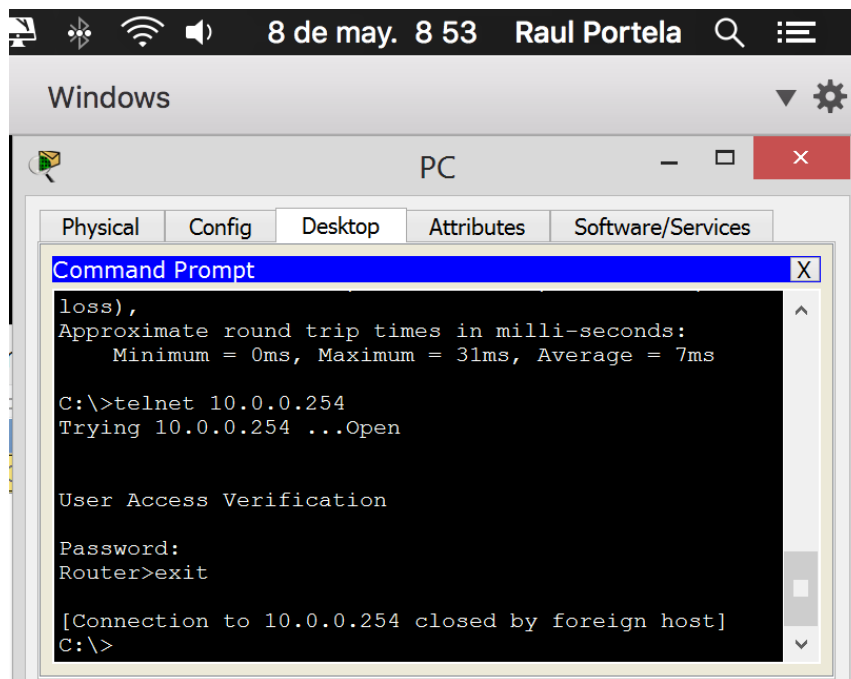
Pinging 10.0.0.254 with 32 bytes of data:

Reply from 10.0.0.254: bytes=32 time=31ms TTL=255
Reply from 10.0.0.254: bytes=32 time<1ms TTL=255
Reply from 10.0.0.254: bytes=32 time<1ms TTL=255
Reply from 10.0.0.254: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 31ms, Average = 7ms

C:\>
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 31ms, Average = 7ms

C:\>telnet 10.0.0.254
Trying 10.0.0.254 ...Open

User Access Verification

Password:
Router>exit

[Connection to 10.0.0.254 closed by foreign host]
C:\>
```

Activity Results

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



64% 8 8 de may. 9 42 Raul Portela

Windows

Cisco Packet Tracer - \\Mac\Home\Documents\Ing Electronica\DIPLOM... - [X]

File Edit Options View Tools Extensions Help

Activity Results Time Elapsed: 00:52:34

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

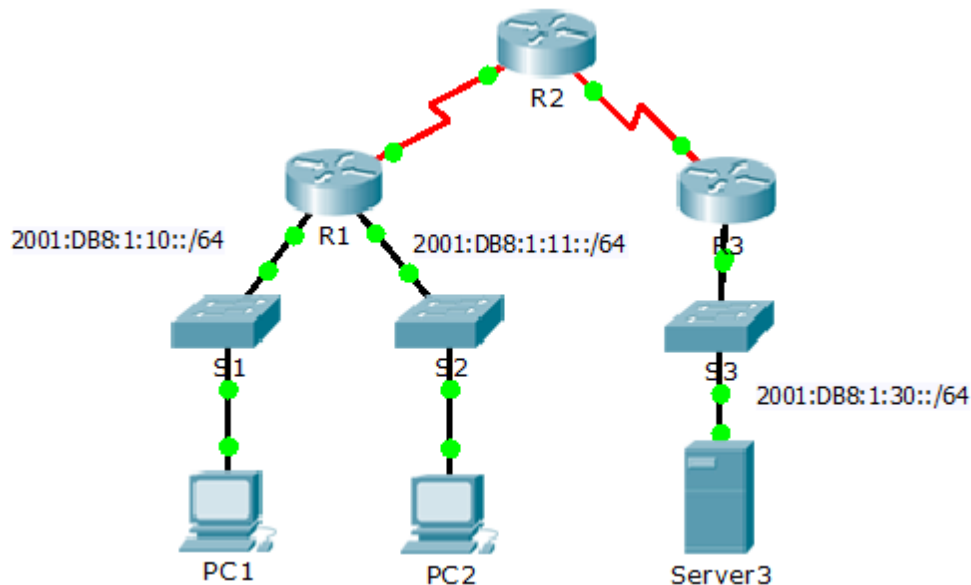
Expand/Collapse All

Assessment Items	Status	Poin	Compon
Network			
Router			
ACL		0	ACL
99	Correct	70	IPv4 S...
VTY Lines			
VTY Line 0		0	Physical
Access ...	Correct	6	IPv4 S...
VTY Line 1		0	Physical
Access ...	Correct	6	IPv4 S...
VTY Line 2		0	Physical

Component	Items/Total	Score
IPv4 Standard ACL Implementation	6/6	100/100

Laboratorio 9.5.2.6 Packet Tracer - Configuring IPv6 ACLs

Topology



Addressing Table

Device	Interface	IPv6 Address/Prefix	Default Gateway
Server3	NIC	2001:DB8:1:30::30/64	FE80::30

Objectives

Part 1: Configure, Apply, and Verify an IPv6 ACL

Part 2: Configure, Apply, and Verify a Second IPv6 ACL

Part 1: Configure, Apply, and Verify an IPv6 ACL

Logs indicate that a computer on the 2001:DB8:1:11::0/64 network is repeatedly refreshing their web page causing a Denial-of-Service (DoS) attack against **Server3**. Until the client can be identified and cleaned, you must block HTTP and HTTPS access to that network with an access list.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Step 1: Configure an ACL that will block HTTP and HTTPS access.

Configure an ACL named **BLOCK_HTTP** on **R1** with the following statements.

a. Block HTTP and HTTPS traffic from reaching **Server3**.

```
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq www
```

```
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq 443
```

b. Allow all other IPv6 traffic to pass.

```
R1(config)# permit ipv6 any any
```



Physical Config CLI

IOS Command Line Interface

```
R1>enable
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 access-list BLOCK_HTTP
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq www
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq 443
R1(config-ipv6-acl)#permit ipv6 any any
R1(config-ipv6-acl)#end
R1#
```

Step 2: Apply the ACL to the correct interface.

Apply the ACL on the interface closest the source of the traffic to be blocked.

```
R1(config)# interface GigabitEthernet0/1
```

```
R1(config-if)# ipv6 traffic-filter BLOCK_HTTP in
```



Physical Config CLI

IOS Command Line

```
R1(config)#ipv6 access-list BLOCK_HTTP
R1(config-ipv6-acl)#interface g0/1
R1(config-if)#ipv6 traffic-filter BLOCK_HTTP in
```

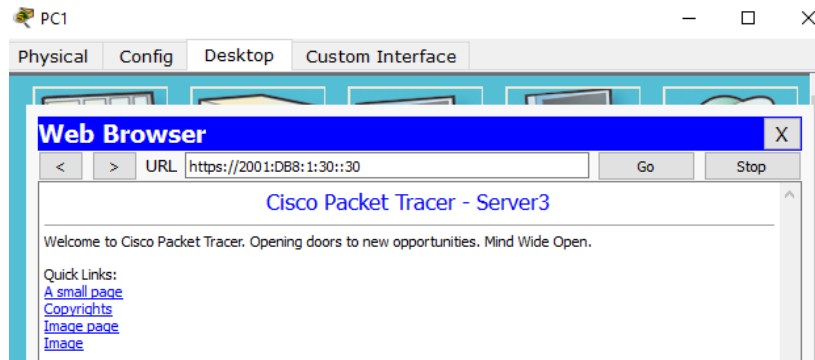
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



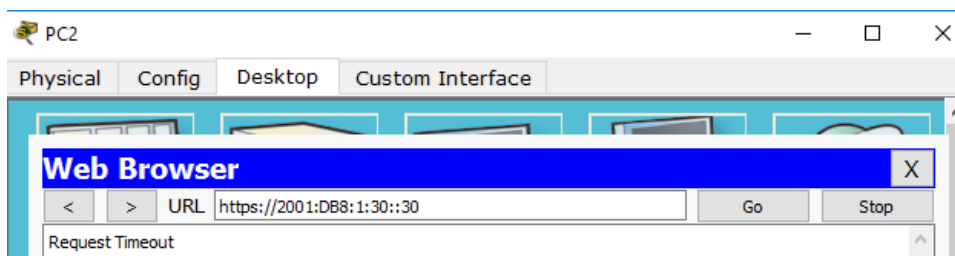
Step 3: Verify the ACL implementation.

Verify the ACL is operating as intended by conducting the following tests:

- Open the **web browser** of **PC1** to `http://2001:DB8:1:30::30` or `https://2001:DB8:1:30::30`. The website should appear.

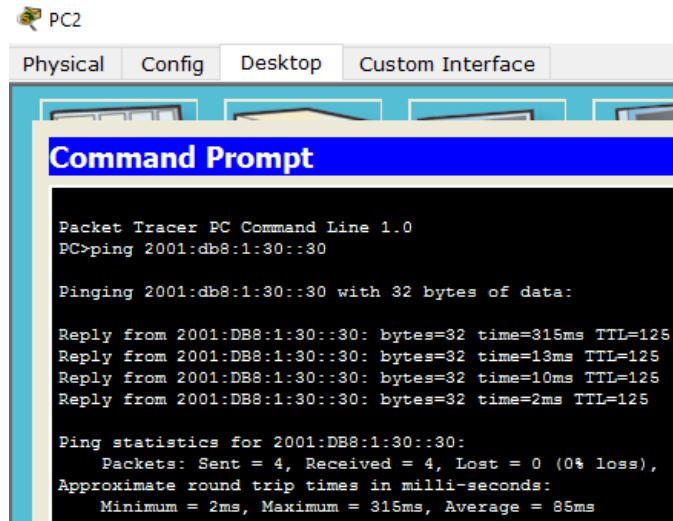


- Open the **web browser** of **PC2** to `http://2001:DB8:1:30::30` or `https://2001:DB8:1:30::30`. The website should be blocked



- Ping from **PC2** to `2001:DB8:1:30::30`. The ping should be successful.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
 Escuela de ciencias básicas tecnologías e Ingeniería
 DIPLOMADO DE PROFUNDIZACION CISCO
 2017 I

```

PC2
Physical Config Desktop Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 2001:db8:1:30::30

Pinging 2001:db8:1:30::30 with 32 bytes of data:

Reply from 2001:DB8:1:30::30: bytes=32 time=315ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=13ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=10ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 315ms, Average = 85ms
  
```

Part 2: Configure, Apply, and Verify a Second IPv6 ACL

The logs now indicate that your server is receiving pings from many different IPv6 addresses in a Distributed Denial of Service (DDoS) attack. You must filter ICMP ping requests to your server.

Step 1: Create an access list to block ICMP.

Configure an ACL named **BLOCK_ICMP** on **R3** with the following statements:

a. Block all ICMP traffic from any hosts to any destination.

```
R3(config)# deny icmp any any
```

b. Allow all other IPv6 traffic to pass.

```
R3(config)# permit ipv6 any any
```

Step 2: Apply the ACL to the correct interface.

In this case, ICMP traffic can come from any source. To ensure that ICMP traffic is blocked regardless of its source or changes that occur to the network topology, apply the ACL closest to the destination.

```

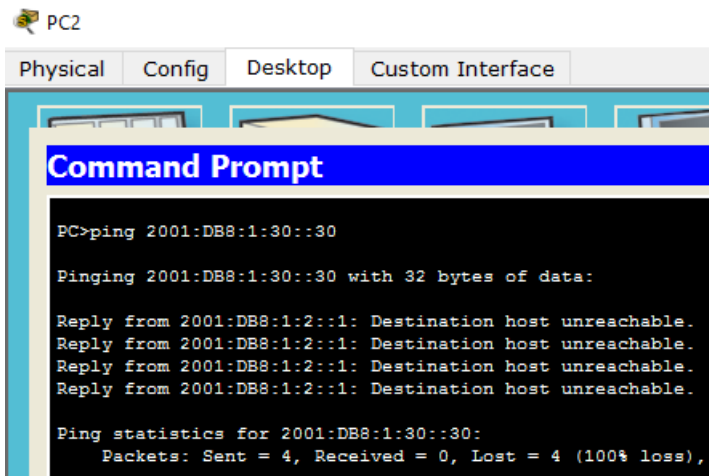
R3(config)# interface GigabitEthernet0/0
R3(config-if)# ipv6 traffic-filter BLOCK_ICMP out
  
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Step 3: Verify that the proper access list functions.

a. Ping from **PC2** to 2001:DB8:1:30::30. The ping should fail.



PC2

Physical Config Desktop Custom Interface

Command Prompt

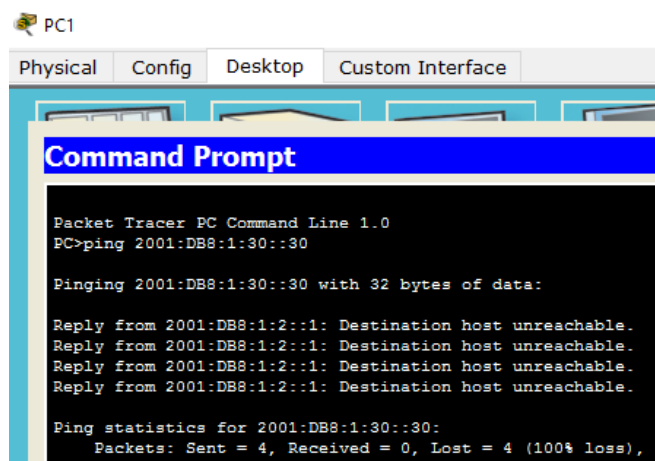
```
PC>ping 2001:DB8:1:30::30

Pinging 2001:DB8:1:30::30 with 32 bytes of data:

Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

b. Ping from **PC1** to 2001:DB8:1:30::30. The ping should fail.



PC1

Physical Config Desktop Custom Interface

Command Prompt

```
Packet Tracer PC Command Line 1.0
PC>ping 2001:DB8:1:30::30

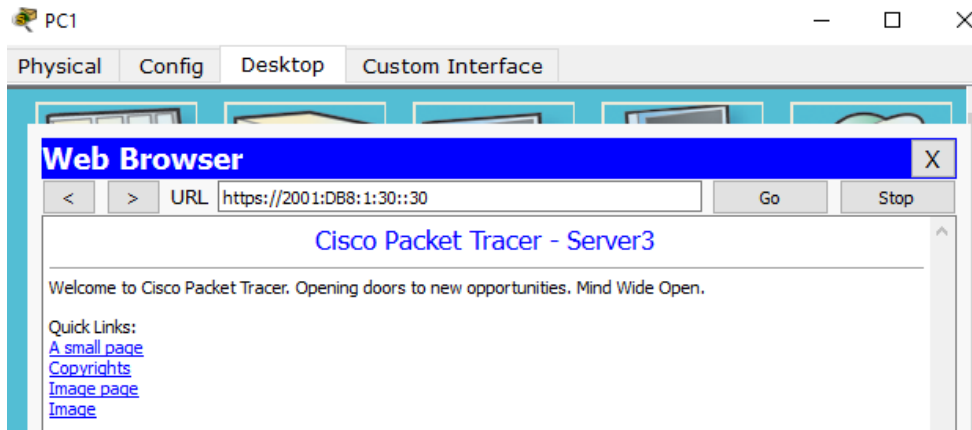
Pinging 2001:DB8:1:30::30 with 32 bytes of data:

Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Open the **web browser** of **PC1** to <http://2001:DB8:1:30::30> or <https://2001:DB8:1:30::30>. The website should display.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Evidencias de la actividad:

Cisco Packet Tracer Student - C:\Users\joseb\Desktop\UNAD\Diplotado de Profundización Cisco\Componente practico\CCNA2 R&S UNIDAD 4\LISTAS DE ACCESO\9.5.2.6 Packet Tracer - Configuring IPv6 ACLs.pka

File Edit Options View Tools Extensions Help

Activity Results

Time Elapsed: 01:05:07

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Points	Component(s)	Feedback
Network				
R1				
ACL V6				
BLOCK_HTTP	Correct	0	ACL	
BLOCK_HTTP		40	IPv6 ACL Impl...	
Ports				
GigabitEthernet0/1		0	Other	
IPv6 Traffic Filter...	Correct	10	IPv6 ACL Impl...	
R3				
ACL V6				
BLOCK_ICMP	Correct	0	ACL	
BLOCK_ICMP		40	IPv6 ACL Impl...	
Ports				
GigabitEthernet0/0		0	Other	
IPv6 Traffic Filter...	Correct	10	IPv6 ACL Impl...	

Component	Items/Total	Score
IPv6 ACL Implementation	4/4	100/100

Score : 100/100
Item Count : 4/4

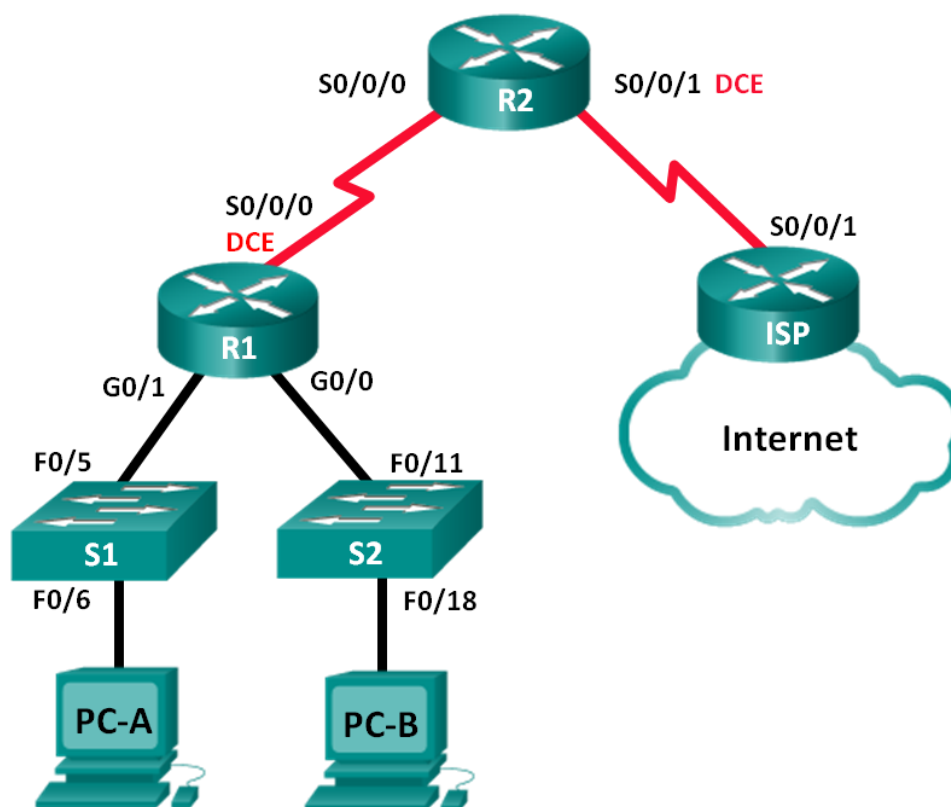
Close

10:23 p. m. 10/05/2017

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

Laboratorio 10.1.2.4 configuración de DHCPv4 básico en un router

Topología



UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.2.253	255.255.255.252	N/A
R2	S0/0/0	192.168.2.254	255.255.255.252	N/A
	S0/0/1 (DCE)	209.165.200.26	255.255.255.24	N/A
ISP	S0/0/1	209.165.200.25	255.255.255.24	N/A
PC-A	NIC	DHCP	DHCP	DHCP
PC-B	NIC	DHCP	DHCP	DHCP

Objetivos

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

Parte 2: configurar un servidor de DHCPv4 y un agente de retransmisión DHCP

Información básica/situación

El protocolo de configuración dinámica de host (DHCP) es un protocolo de red que permite a los administradores de red administrar y automatizar la asignación de direcciones IP. Sin DHCP, el administrador debe asignar y configurar manualmente las direcciones IP, los servidores DNS preferidos y los gateways predeterminados. A medida que aumenta el tamaño de la red, esto se convierte en un problema administrativo cuando los dispositivos se trasladan de una red interna a otra.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



En esta situación, la empresa creció en tamaño, y los administradores de red ya no pueden asignar direcciones IP a los dispositivos de forma manual. Su tarea es configurar el router R2 para asignar direcciones IPv4 en dos subredes diferentes conectadas al router R1.

Nota: en esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos que efectivamente se necesitan para configurar DHCP. Sin embargo, los comandos requeridos se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar los dispositivos sin consultar el apéndice.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios

3 ROUTERS (CISCO 1941 CON IOS DE CISCO VERSIÓN 15.2(4)M3, IMAGEN UNIVERSAL O SIMILAR)

2 SWITCHES (CISCO 2960 CON IOS DE CISCO VERSIÓN 15.0(2), IMAGEN LANBASEK9 O SIMILAR)

2 COMPUTADORAS (WINDOWS 7, VISTA O XP CON UN PROGRAMA DE EMULACIÓN DE TERMINAL, COMO TERA TERM)

CABLES DE CONSOLA PARA CONFIGURAR LOS DISPOSITIVOS CON IOS DE CISCO MEDIANTE LOS PUERTOS DE CONSOLA

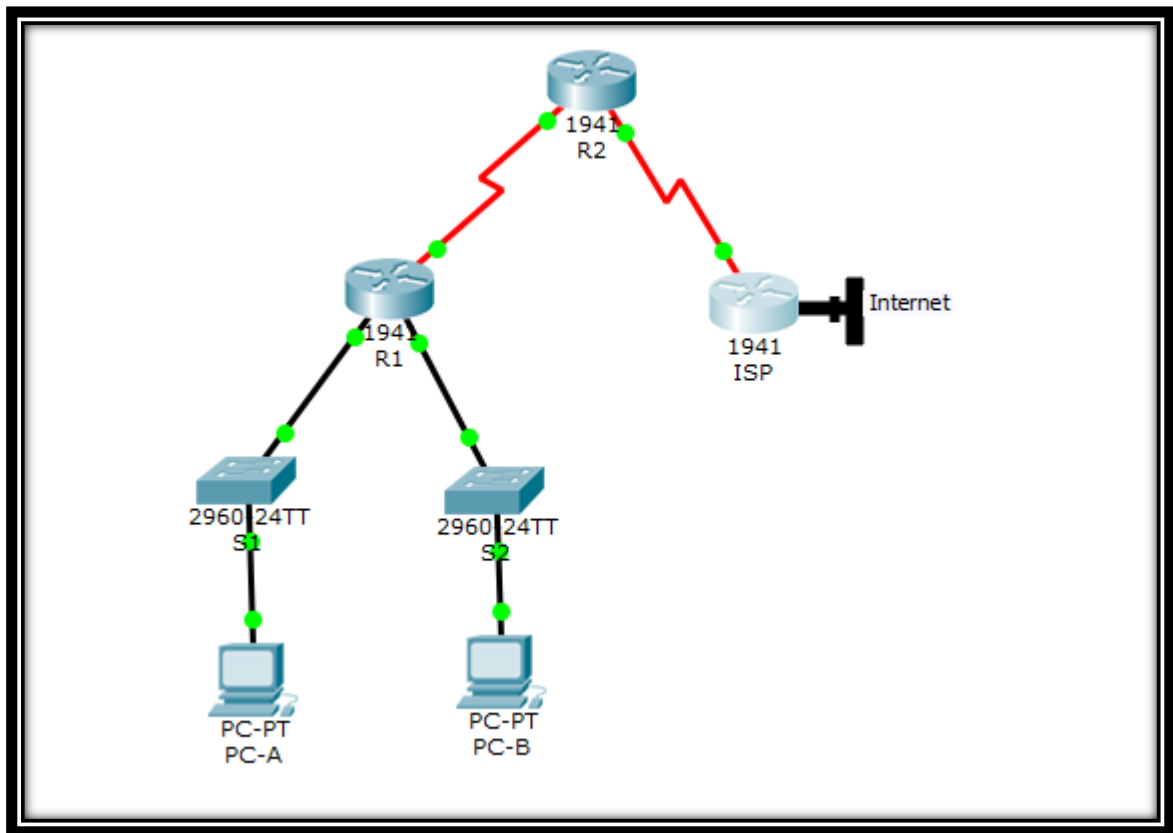
CABLES ETHERNET Y SERIALES, COMO SE MUESTRA EN LA TOPOLOGÍA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

Parte 2. armar la red y configurar los parámetros básicos de los dispositivos

En la parte 1, establecerá la topología de la red y configurará los routers y switches con los parámetros básicos, como las contraseñas y las direcciones IP. Además, configurará los parámetros de IP de las computadoras en la topología.

Paso 1. realizar el cableado de red tal como se muestra en la topología.



Paso 2. inicializar y volver a cargar los routers y los switches.

Paso 3. configurar los parámetros básicos para cada router.

- Desactive la búsqueda DNS.
- Configure el nombre del dispositivo como se muestra en la topología.
- Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



- d. Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- e. Configure **logging synchronous** para evitar que los mensajes de consola interrumpen la entrada de comandos.
- f. Configure las direcciones IP para todas las interfaces de los routers de acuerdo con la tabla de direccionamiento.
- g. Configure la interfaz DCE serial en el R1 y el R2 con una frecuencia de reloj de 128000.
- h. Configure EIGRP for R1.
R1(config)# **router eigrp 1**
R1(config-router)# **network 192.168.0.0 0.0.0.255**
R1(config-router)# **network 192.168.1.0 0.0.0.255**
R1(config-router)# **network 192.168.2.252 0.0.0.3**
R1(config-router)# **no auto-summary**
- i. Configure EIGRP y una ruta predeterminada al ISP en el R2.
R2(config)# **router eigrp 1**
R2(config-router)# **network 192.168.2.252 0.0.0.3**
R2(config-router)# **redistribute static**
R2(config-router)# **exit**
R2(config)# **ip route 0.0.0.0 0.0.0.0 209.165.200.225**
- j. Configure una ruta estática resumida en el ISP para llegar a las redes en los routers R1 y R2.
ISP(config)# **ip route 192.168.0.0 255.255.252.0 209.165.200.226**
- k. Copie la configuración en ejecución en la configuración de inicio

Paso 4. verificar la conectividad de red entre los routers.

Si algún ping entre los routers falla, corrija los errores antes de continuar con el siguiente paso. Use los comandos show ip route y show ip interface brief para detectar posibles problemas.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Paso 5. verificar que los equipos host estén configurados para DHCP.

Parte 3. configurar un servidor de DHCPv4 y un agente de retransmisión DHCP

Para asignar automáticamente la información de dirección en la red, configure el R2 como servidor de DHCPv4 y el R1 como agente de retransmisión DHCP.

Paso 1. configurar los parámetros del servidor de DHCPv4 en el router R2.

En el R2, configure un conjunto de direcciones DHCP para cada LAN del R1. Utilice el nombre de conjunto R1G0 para G0/0 LAN y R1G1 para G0/1 LAN. Asimismo, configure las direcciones que se excluirán de los conjuntos de direcciones. La práctica recomendada indica que primero se deben configurar las direcciones excluidas, a fin de garantizar que no se arrienden accidentalmente a otros dispositivos.

Excluya las primeras nueve direcciones en cada LAN del R1; empiece por .1. El resto de las direcciones deben estar disponibles en el conjunto de direcciones DHCP. Asegúrese de que cada conjunto de direcciones DHCP incluya un gateway predeterminado, el dominio ccna-lab.com, un servidor DNS (209.165.200.225) y un tiempo de arrendamiento de dos días.

En las líneas a continuación, escriba los comandos necesarios para configurar los servicios DHCP en el router R2, incluso las direcciones DHCP excluidas y los conjuntos de direcciones DHCP.

Nota: los comandos requeridos para la parte 2 se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar DHCP en el R1 y el R2 sin consultar el apéndice.

```
R2(config)# ip dhcp excluded-address 192.168.0.1 192.168.0.9
```

```
R2(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.9
```

```
R2(config)# ip dhcp pool R1G1
```

```
R2(dhcp-config)# network 192.168.1.0 255.255.255.0
```

```
R2(dhcp-config)# default-router 192.168.1.1
```

```
R2(dhcp-config)# dns-server 209.165.200.225
```

```
R2(dhcp-config)# domain-name ccna-lab.com
```

```
R2(dhcp-config)# lease 2
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
R2(dhcp-config)# exit
R2(config)# ip dhcp pool R1G0
R2(dhcp-config)# network 192.168.0.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.0.1
R2(dhcp-config)# dns-server 209.165.200.225
R2(dhcp-config)# domain-name ccna-lab.com
R2(dhcp-config)# lease 2
```

En la PC-A o la PC-B, abra un símbolo del sistema e introduzca el comando ipconfig /all. ¿Alguno de los equipos host recibió una dirección IP del servidor de DHCP? ¿Por qué?

Los equipos host no reciben IP del servidor de DHCP en el R2 hasta que el R1 esté configurado

Paso 2. configurar el R1 como agente de retransmisión DHCP.

Configure las direcciones IP de ayuda en el R1 para que reenvíen todas las solicitudes de DHCP al servidor de DHCP en el R2.

En las líneas a continuación, escriba los comandos necesarios para configurar el R1 como agente de retransmisión DHCP para las LAN del R1.

```
R1(config)# interface g0/0
R1(config-if)# ip helper-address 192.168.2.254
R1(config-if)# exit
R1(config)# interface g0/1
R1(config-if)# ip helper-address 192.168.2.254
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
R1(config)#interface g0/0
R1(config-if)#ip helper-address 192.168.2.254
R1(config-if)#exit
R1(config)#interface g0/1
R1(config-if)#ip helper-address 192.168.2.254
R1(config-if)#exit
R1(config)#exit
R1#
```

Paso 3. registrar la configuración IP para la PC-A y la PC-B.

En la PC-A y la PC-B, emita el comando `ipconfig /all` para verificar que las computadoras recibieron la información de la dirección IP del servidor de DHCP en el R2. Registre la dirección IP y la dirección MAC de cada computadora.

Respuesta puede ser variable

Según el pool de DHCP que se configuró en el R2, ¿cuáles son las primeras direcciones IP disponibles que la PC-A y la PC-B pueden arrendar?

PC-B: 192.168.0.10 y PC-A: 192.168.1.10

Paso 4. verificar los servicios DHCP y los arrendamientos de direcciones en el R2.

- En el R2, introduzca el comando `show ip dhcp binding` para ver los arrendamientos de direcciones DHCP.

R2# show ip dhcp binding

Bindings from all pools not associated with VRF:

IP address	Client-ID/ Hardware address/ User name	Lease expiration	Type
192.168.0.10	011c.c1de.91c3.5d	Mar 13 2013 02:07 AM	Automatic
192.168.1.10	0100.2170.0c05.0c	Mar 13 2013 02:09 AM	Automatic

Junto con las direcciones IP que se arrendaron, ¿qué otra información útil de identificación de cliente aparece en el resultado?

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Las direcciones de hardware del cliente permiten identificar las computadoras específicas que se unieron a la red.

- b. En el R2, introduzca el comando **show ip dhcp server statistics** para ver la actividad de mensajes y las estadísticas del pool de DHCP.

R2# show ip dhcp server statistics

Memory usage 42175
Address pools 2
Database agents 0
Automatic bindings 2
Manual bindings 0
Expired bindings 0
Malformed messages 0
Secure arp entries 0

Message	Received
BOOTREQUEST	0
DHCPDISCOVER	2
DHCPREQUEST	2
DHCPDECLINE	0
DHCPRELEASE	0
DHCPINFORM	2

Message	Sent
BOOTREPLY	0
DHCPOFFER	2
DHCPACK	4
DHCPNAK	0

¿Cuántos tipos de mensajes DHCP se indican en el resultado?

10

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



- c. En el R2, introduzca el comando **show ip dhcp pool** para ver la configuración del pool de DHCP.

R2# show ip dhcp pool

Pool R1G1 :

Utilization mark (high/low) : 100 / 0

Subnet size (first/next) : 0 / 0

Total addresses : 254

Leased addresses : 1

Pending event : none

1 subnet is currently in the pool :

Current index	IP address range	Leased addresses
192.168.1.11	192.168.1.1 - 192.168.1.254	1

Pool R1G0 :

Utilization mark (high/low) : 100 / 0

Subnet size (first/next) : 0 / 0

Total addresses : 254

Leased addresses : 1

Pending event : none

1 subnet is currently in the pool :

Current index	IP address range	Leased addresses
192.168.0.11	192.168.0.1 - 192.168.0.254	1

En el resultado del comando **show ip dhcp pool**, ¿a qué hace referencia el índice actual (Current index)?

Dirección disponible para arrendamiento

- d. En el R2, introduzca el comando **show run | section dhcp** para ver la configuración DHCP en la configuración en ejecución.

R2# show run | section dhcp

ip dhcp excluded-address 192.168.0.1 192.168.0.9

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
ip dhcp excluded-address 192.168.1.1 192.168.1.9
ip dhcp pool R1G1
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 domain-name ccna-lab.com
 dns-server 209.165.200.225
 lease 2
ip dhcp pool R1G0
 network 192.168.0.0 255.255.255.0
 default-router 192.168.0.1
 domain-name ccna-lab.com
 dns-server 209.165.200.225
 lease 2
```

- e. En el R2, introduzca el comando **show run interface** para las interfaces G0/0 y G0/1 para ver la configuración de retransmisión DHCP en la configuración en ejecución.

```
R2# show run interface g0/0
Building configuration...
```

```
Current configuration : 132 bytes
!
interface GigabitEthernet0/0
ip address 192.168.0.1 255.255.255.0
ip helper-address 192.168.2.254
duplex auto
speed auto
end
```

```
R2# show run interface g0/1
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Building configuration...

Current configuration : 132 bytes

!

interface GigabitEthernet0/1

ip address 192.168.1.1 255.255.255.0

ip helper-address 192.168.2.254

duplex auto

speed auto

end

Reflexión

¿Cuál cree que es el beneficio de usar agentes de retransmisión DHCP en lugar de varios routers que funcionen como servidores de DHCP?

Con este tipo de servidor y ruter independientes para cada subred ara mas dificultosa la administración , y forzara a cada Router a administrar los direccionamientos DHCP .

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet n.º 2	Interfaz serial #1	Interfaz serial n.º 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

Laboratorio 10.1.2.5 configuración de DHCPv4 básico en un switch

Topología

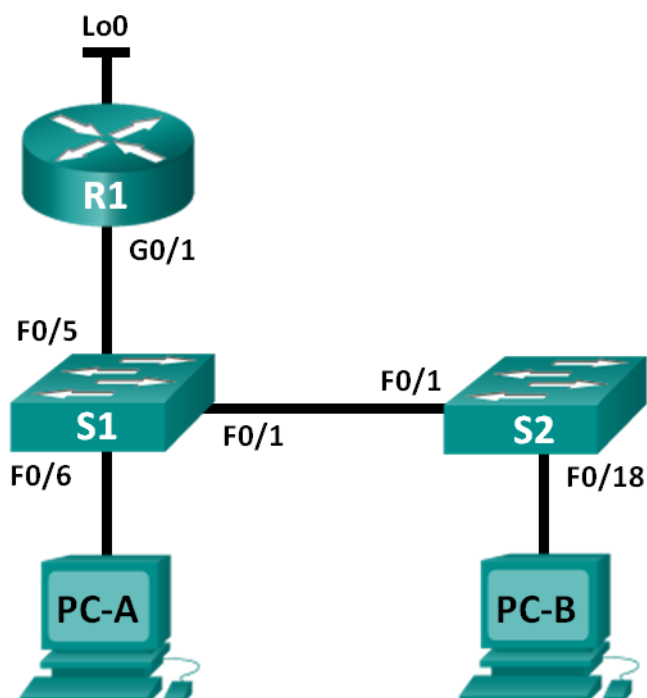


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	G0/1	192.168.1.10	255.255.255.0
	Lo0	209.165.200.225	255.255.255.224
S1	VLAN 1	192.168.1.1	255.255.255.0
	VLAN 2	192.168.2.1	255.255.255.0

Objetivos

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

Parte 2: cambiar la preferencia de SDM

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



ESTABLECER LA PREFERENCIA DE SDM EN LANBASE-ROUTING EN EL S1.

Parte 3: configurar DHCPv4

CONFIGURAR DHCPV4 PARA LA VLAN 1.

VERIFICAR LA CONECTIVIDAD Y DHCPV4.

Parte 4: configurar DHCP para varias VLAN

ASIGNAR PUERTOS A LA VLAN 2.

CONFIGURAR DHCPV4 PARA LA VLAN 2.

VERIFICAR LA CONECTIVIDAD Y DHCPV4.

Parte 5: habilitar el routing IP

HABILITE EL ROUTING IP EN EL SWITCH.

CREAR RUTAS ESTÁTICAS.

Información básica/situación

Un switch Cisco 2960 puede funcionar como un servidor de DHCPv4. El servidor de DHCPv4 de Cisco asigna y administra direcciones IPv4 de conjuntos de direcciones identificados que están asociados a VLAN específicas e interfaces virtuales de switch (SVI). El switch Cisco 2960 también puede funcionar como un dispositivo de capa 3 y hacer routing entre VLAN y una cantidad limitada de rutas estáticas. En esta práctica de laboratorio, configurará DHCPv4 para VLAN únicas y múltiples en un switch Cisco 2960, habilitará el routing en el switch para permitir la comunicación entre las VLAN y agregará rutas estáticas para permitir la comunicación entre todos los hosts.

Nota: en esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos que efectivamente se necesitan para configurar DHCP. Sin embargo, los comandos requeridos se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar los dispositivos sin consultar el apéndice.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

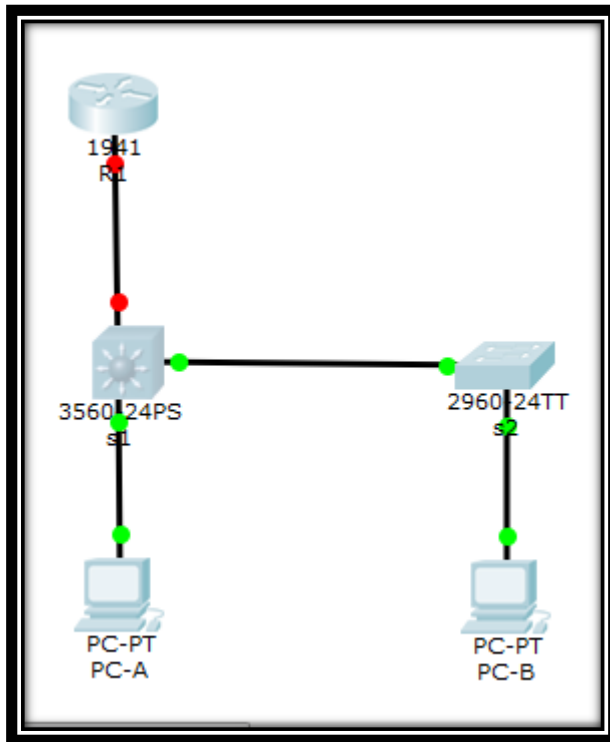
Nota: asegúrese de que el router y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios

- 1 ROUTER (CISCO 1941 CON IOS DE CISCO VERSIÓN 15.2(4)M3, IMAGEN UNIVERSAL O SIMILAR)**
- 2 SWITCHES (CISCO 2960 CON IOS DE CISCO VERSIÓN 15.0(2), IMAGEN LANBASEK9 O SIMILAR)**
- 2 COMPUTADORAS (WINDOWS 7, VISTA O XP CON UN PROGRAMA DE EMULACIÓN DE TERMINAL, COMO TERA TERM)**
- CABLES DE CONSOLA PARA CONFIGURAR LOS DISPOSITIVOS CON IOS DE CISCO MEDIANTE LOS PUERTOS DE CONSOLA**
- CABLES ETHERNET, COMO SE MUESTRA EN LA TOPOLOGÍA**

Parte 4: armar la red y configurar los parámetros básicos de los dispositivos

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Paso 1: realizar el cableado de red tal como se muestra en la topología.

Paso 2: inicializar y volver a cargar los routers y switches.

Paso 3: configurar los parámetros básicos en los dispositivos.

- Asigne los nombres de dispositivos como se muestra en la topología.
- Desactive la búsqueda del DNS.
- Asigne **class** como la contraseña de enable y asigne **cisco** como la contraseña de consola y la contraseña de vty.
- Configure las direcciones IP en las interfaces G0/1 y Lo0 del R1, según la tabla de direccionamiento.
- Configure las direcciones IP en las interfaces VLAN 1 y VLAN 2 del S1, según la tabla de direccionamiento.
- Guarde la configuración en ejecución en el archivo de configuración de inicio.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
R1(config)#INT G0/1
R1(config-if)#IP 192.168.1.10 255.255.255.0
^
% Invalid input detected at '^' marker.
R1(config-if)#ip 192.168.1.10 255.255.255.0
^
% Invalid input detected at '^' marker.
R1(config-if)#ip add 192.168.1.10 255.255.255.0
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
to up

R1(config-if)#int lo0

R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R1(config-if)#ip add 209.165.200.225 255.255.255.224
R1(config-if)#no shut
R1(config-if)#
```

```
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to
up

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to
up

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#host s1
s1(config)#int vlan 1
s1(config-if)#ip add 192.168.1.1 255.255.255.0
s1(config-if)#no shut

s1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```


UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
s1>en
s1#conf t
Enter configuration commands, one per line. End with
s1(config)#int vlan 2
s1(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2,
s1(config-if)#exit
s1(config)#int vlan 2
s1(config-if)#ip add 192.168.2.1 255.255.0
^
% Invalid input detected at '^' marker.

s1(config-if)#ip add 192.168.2.1 255.255.255.0
s1(config-if)#no shut
s1(config-if)#exit
s1(config)#
```

Parte 5: cambiar la preferencia de SDM

Switch Database Manager (SDM) de Cisco proporciona varias plantillas para el switch Cisco 2960. Las plantillas pueden habilitarse para admitir funciones específicas según el modo en que se utilice el switch en la red. En esta práctica de laboratorio, la plantilla lanbase-routing está habilitada para permitir que el switch realice el routing entre VLAN y admita el routing estático.

Paso 1: mostrar la preferencia de SDM en el S1.

En el S1, emita el comando show sdm prefer en modo EXEC privilegiado. Si no se cambió la plantilla predeterminada de fábrica, debería seguir siendo default. La plantilla default no admite routing estático. Si se habilitó el direccionamiento IPv6, la plantilla será dual-ipv4-and-ipv6 default.

```
S1# show sdm prefer
The current template is "default" template.
The selected template optimizes the resources in
the switch to support this level of features for
0 routed interfaces and 255 VLANs.
```

number of unicast mac addresses:	8K
number of IPv4 IGMP groups:	0.25K

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```

number of IPv4/MAC qos aces:          0.125k
number of IPv4/MAC security aces:     0.375k

```

ejecutando el commando

S1# show sdm prefer

*The current template is "dual-ipv4-and-ipv6 default" template.
The selected template optimizes the resources in
the switch to support this level of features for
0 routed interfaces and 255 VLANs.*

```

number of unicast mac addresses:      4K
number of IPv4 IGMP groups + multicast routes: 0.25K
number of IPv4 unicast routes:       0
number of IPv6 multicast groups:     0.375k
number of directly-connected IPv6 addresses: 0
number of indirect IPv6 unicast routes: 0
number of IPv4 policy based routing aces: 0
number of IPv4/MAC qos aces:         0.125k
number of IPv4/MAC security aces:    0.375k
number of IPv6 policy based routing aces: 0
number of IPv6 qos aces:             0.625k
number of IPv6 security aces:        125

```

S1# show sdm prefer

*The current template is "lanbase-routing" template.
The selected template optimizes the resources in
the switch to support this level of features for
0 routed interfaces and 255 VLANs.*

```

number of unicast mac addresses:      4K
number of IPv4 IGMP groups + multicast routes: 0.25K
number of IPv4 unicast routes:       0.75K
    number of directly-connected IPv4 hosts: 0.75K
    number of indirect IPv4 routes:      16
number of IPv6 multicast groups:     0.375k
number of directly-connected IPv6 addresses: 0.75K
    number of indirect IPv6 unicast routes: 16
number of IPv4 policy based routing aces: 0
number of IPv4/MAC qos aces:         0.125k
number of IPv4/MAC security aces:    0.375k
number of IPv6 policy based routing aces: 0
number of IPv6 qos aces:             0.375k

```

number of IPv6 security aces: 127

¿Cuál es la plantilla actual?

lanbase-routing

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Paso 2: cambiar la preferencia de SDM en el S1.

- a. Establezca la preferencia de SDM en **lanbase-routing**. (Si lanbase-routing es la plantilla actual, continúe con la parte 3). En el modo de configuración global, emita el comando **sdm prefer lanbase-routing**.

```
S1(config)# sdm prefer lanbase-routing
```

Changes to the running SDM preferences have been stored, but cannot take effect until the next reload.

Use 'show sdm prefer' to see what SDM preference is currently active.

```
S1# show sdm prefer
```

The current template is "default" template.

The selected template optimizes the resources in the switch to support this level of features for 0 routed interfaces and 255 VLANs.

<i>number of unicast mac addresses:</i>	<i>8K</i>
<i>number of IPv4 IGMP groups:</i>	<i>0.25K</i>
<i>number of IPv4/MAC qos aces:</i>	<i>0.125k</i>
<i>number of IPv4/MAC security aces:</i>	<i>0.375k</i>

On next reload, template will be "lanbase-routing" template.

¿Qué plantilla estará disponible después de la recarga?

Lanbase-routing

- b. Se debe volver a cargar el switch para que la plantilla esté habilitada.

```
S1# reload
```

System configuration has been modified. Save? [yes/no]: **no**

Proceed with reload? [confirm]

Nota: la nueva plantilla se utilizará después del reinicio, incluso si no se guardó la configuración en ejecución. Para guardar la configuración en ejecución, responda **yes** (sí) para guardar la configuración modificada del sistema.

Paso 3: verificar que la plantilla lanbase-routing esté cargada.

Emita el comando show sdm prefer para verificar si la plantilla lanbase-routing se cargó en el S1.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
S1# show sdm prefer
```

```
The current template is "lanbase-routing" template.  
The selected template optimizes the resources in  
the switch to support this level of features for  
0 routed interfaces and 255 VLANs.
```

```
number of unicast mac addresses:          4K  
number of IPv4 IGMP groups + multicast routes: 0.25K  
number of IPv4 unicast routes:           0.75K  
    number of directly-connected IPv4 hosts: 0.75K  
    number of indirect IPv4 routes:        16  
number of IPv6 multicast groups:          0.375k  
number of directly-connected IPv6 addresses: 0.75K  
    number of indirect IPv6 unicast routes: 16  
number of IPv4 policy based routing aces: 0  
number of IPv4/MAC qos aces:              0.125k  
number of IPv4/MAC security aces:         0.375k  
number of IPv6 policy based routing aces: 0  
number of IPv6 qos aces:                  0.375k  
number of IPv6 security aces:             127
```

Parte 6: configurar DHCPv4

En la parte 3, configurará DHCPv4 para la VLAN 1, revisará las configuraciones IP en los equipos host para validar la funcionalidad de DHCP y verificará la conectividad de todos los dispositivos en la VLAN 1.

Paso 1: configurar DHCP para la VLAN 1.

- Excluya las primeras 10 direcciones host válidas de la red 192.168.1.0/24. En el espacio proporcionado, escriba el comando que utilizó.

```
S1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10
```

- Cree un pool de DHCP con el nombre **DHCP1**. En el espacio proporcionado, escriba el comando que utilizó.

```
S1(config)# ip dhcp pool DHCP1
```

- Asigne la red 192.168.1.0/24 para las direcciones disponibles. En el espacio proporcionado, escriba el comando que utilizó.

```
S1(dhcp-config)# network 192.168.1.0 255.255.255.0
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



- d. Asigne el gateway predeterminado como 192.168.1.1. En el espacio proporcionado, escriba el comando que utilizó.

S1(dhcp-config)# default-router 192.168.1.1

- e. Asigne el servidor DNS como 192.168.1.9. En el espacio proporcionado, escriba el comando que utilizó.

S1(dhcp-config)# dns-server 192.168.1.9

- f. Asigne un tiempo de arrendamiento de tres días. En el espacio proporcionado, escriba el comando que utilizó.

S1(dhcp-config)# lease 3...no valido

- g. Guarde la configuración en ejecución en el archivo de configuración de inicio.

```

S1(config)#int vlan 2
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up

S1(config-if)#exit
S1(config)#int vlan 2
S1(config-if)#ip add 192.168.2.1 255.255.0
^
% Invalid input detected at '^' marker.

S1(config-if)#ip add 192.168.2.1 255.255.255.0
S1(config-if)#no shut
S1(config-if)#exit
S1(config)#ip excluded-address 192.168.1.1 192.168.1.10
^
% Invalid input detected at '^' marker.

S1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
^
% Invalid input detected at '^' marker.

S1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
S1(config)#ip dhcp pool dhcp1
S1(dhcp-config)#network 192.168.1.0 255.255.255.0
S1(dhcp-config)#default-router 192.168.1.1
S1(dhcp-config)#dns-server 192.168.1.9
S1(dhcp-config)#

```

- h.

Paso 2: verificar la conectividad y DHCP.

- a. En la PC-A y la PC-B, abra el símbolo del sistema y emita el comando **ipconfig**. Si la información de IP no está presente, o si está incompleta, emita el comando **ipconfig /release**, seguido del comando **ipconfig /renew**.

Para la PC-A, incluya lo siguiente:

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Dirección IP: _____ **192.168.1.11**
Máscara de subred: _____ **255.255.255.0**
Gateway predeterminado: _____ **192.168.1.1**
Para la PC-B, incluya lo siguiente:
Dirección IP: _____ **192.168.1.12**
Máscara de subred: _____ **255.255.255.0**
Gateway predeterminado: _____ **192.168.1.1**

- b. Pruebe la conectividad haciendo ping de la PC-A al gateway predeterminado, la PC-B y el R1.
¿Es posible hacer ping de la PC-A al gateway predeterminado de la VLAN 1? _____ **SI**
¿Es posible hacer ping de la PC-A a la PC-B? _____ **SI**
¿Es posible hacer ping de la PC-A a la interfaz G0/1 del R1? _____ **SI**

Parte 7: configurar DHCPv4 para varias VLAN

En la parte 4, asignará la PC-A un puerto que accede a la VLAN 2, configurará DHCPv4 para la VLAN 2, renovará la configuración IP de la PC-A para validar DHCPv4 y verificará la conectividad dentro de la VLAN.

Paso 1: asignar un puerto a la VLAN 2.

Coloque el puerto F0/6 en la VLAN 2. En el espacio proporcionado, escriba el comando que utilizó.

Paso 2: configurar DHCPv4 para la VLAN 2.

- a. Excluya las primeras 10 direcciones host válidas de la red 192.168.2.0. En el espacio proporcionado, escriba el comando que utilizó.

S1(config)# interface f0/6

S1(config-if)# switchport access vlan 2

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



- b. Cree un pool de DHCP con el nombre **DHCP2**. En el espacio proporcionado, escriba el comando que utilizó.

S1(config)# ip dhcp pool DHCP2

- c. Asigne la red 192.168.2.0/24 para las direcciones disponibles. En el espacio proporcionado, escriba el comando que utilizó.

S1(dhcp-config)# network 192.168.2.0 255.255.255.0

- d. Asigne el gateway predeterminado como 192.168.2.1. En el espacio proporcionado, escriba el comando que utilizó.

S1(dhcp-config)# default-router 192.168.2.1

- e. Asigne el servidor DNS como 192.168.2.9. En el espacio proporcionado, escriba el comando que utilizó.

S1(dhcp-config)# dns-server 192.168.2.9

- f. Asigne un tiempo de arrendamiento de tres días. En el espacio proporcionado, escriba el comando que utilizó.

S1(dhcp-config)# lease 3

Paso 3: verificar la conectividad y DHCPv4.

- a. En la PC-A, abra el símbolo del sistema y emita el comando **ipconfig /release**, seguido del comando **ipconfig /renew**.

Para la PC-A, incluya lo siguiente:

Dirección IP: _____ **192.168.2.11**

Máscara de subred: _____ **255.255.255.0**

Gateway predeterminado: _____ **192.168.2.1**

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```

Command Prompt

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0002.176C.3625
Link-local IPv6 Address.....: FE80::202:17FF:FE6C:3625
IP Address.....: 192.168.2.11
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.2.1
DNS Servers.....: 192.168.2.9
DHCP Servers.....: 192.168.2.1
DHCPv6 Client DUID.....: 00-01-00-01-71-03-51-E0-00-02-17-6C-36-25

PC>ipconfig /all

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0002.176C.3625
Link-local IPv6 Address.....: FE80::202:17FF:FE6C:3625
IP Address.....: 192.168.2.11
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.2.1
DNS Servers.....: 192.168.2.9
DHCP Servers.....: 192.168.2.1
DHCPv6 Client DUID.....: 00-01-00-01-71-03-51-E0-00-02-17-6C-36-25

PC>

```

- b. Pruebe la conectividad haciendo ping de la PC-A al gateway predeterminado de la VLAN 2 y a la PC-B.

¿Es posible hacer ping de la PC-A al gateway predeterminado? _____ **SI**

¿Es posible hacer ping de la PC-A a la PC-B? _____ **no**

¿Los pings eran correctos? ¿Por qué?

No están haciendo ruteo entre esas dsos direcciones

- c. Emita el comando **show ip route** en el S1.

¿Qué resultado arrojó este comando?

S1# show ip route

Default gateway is not set

Host	Gateway	Last Use	Total Uses	Interface
ICMP redirect cache is empty				

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Parte 8: habilitar el routing IP

En la parte 5, habilitará el routing IP en el switch, que permitirá la comunicación entre VLAN. Para que todas las redes se comuniquen, se deben implementar rutas estáticas en el S1 y el R1.

Paso 1: habilitar el routing IP en el S1.

- En el modo de configuración global, utilice el comando **ip routing** para habilitar el routing en el S1.

```
S1(config)# ip routing
```

- Verificar la conectividad entre las VLAN.

¿Es posible hacer ping de la PC-A a la PC-B? _____ SI

¿Qué función realiza el switch?

El switch hace routing entre VLAN.

Vea la información de la tabla de routing para el S1.

```
S1# show ip route
```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

*ia - IS-IS inter area, * - candidate default, U - per-user static route*

o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

+ - replicated route, % - next hop override

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.1.0/24 is directly connected, Vlan1

L 192.168.1.1/32 is directly connected, Vlan1

192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.2.0/24 is directly connected, Vlan2

L 192.168.2.1/32 is directly connected, Vlan2

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```

s1(config)#ip routing
s1(config)#exit
s1#
%SYS-5-CONFIG_I: Configured from console by console

s1#ip routing
^
% Invalid input detected at '^' marker.

s1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C      192.168.1.0/24 is directly connected, Vlan1
C      192.168.2.0/24 is directly connected, Vlan2
s1#
  
```

¿Qué información de la ruta está incluida en el resultado de este comando?

El switch exhibe una tabla de routing que muestra las VLAN como las redes conectadas directamente 192.168.1.0/24 y 192.168.2.0/24.

- c. Vea la información de la tabla de routing para el R1.

R1# show ip route

**Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override**

Gateway of last resort is not set

**192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
L 192.168.1.10/32 is directly connected, GigabitEthernet0/1**

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



¿Qué información de la ruta está incluida en el resultado de este comando?

El resultado del router muestra las redes conectadas

d. ¿Es posible hacer ping de la PC-A al R1? _____ **NO**

¿Es posible hacer ping de la PC-A a la interfaz Lo0? _____ **NO**

Considere la tabla de routing de los dos dispositivos, ¿qué se debe agregar para que haya comunicación entre todas las redes?

Rutas a las tablas de routing

Paso 2: asignar rutas estáticas.

Habilitar el routing IP permite que el switch enrute entre VLAN asignadas en el switch. Para que todas las VLAN se comuniquen con el router, es necesario agregar rutas estáticas a la tabla de routing del switch y del router.

a. En el S1, cree una ruta estática predeterminada al R1. En el espacio proporcionado, escriba el comando que utilizó.

S1(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.10

```
S1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.10
S1(config)#
```

b. En el R1, cree una ruta estática a la VLAN 2. En el espacio proporcionado, escriba el comando que utilizó.

R1(config)# ip route 192.168.2.0 255.255.255.0 g0/1

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip route 192.168.2.0 255.255.255.0 g0/1
%Default route without gateway, if not a point-to-point interface, may impact
performance
```

c. Vea la información de la tabla de routing para el S1.

¿Cómo está representada la ruta estática predeterminada?

S1# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



*i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override*

Gateway of last resort is 192.168.1.10 to network 0.0.0.0

```
S*    0.0.0.0/0 [1/0] via 192.168.1.10
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.1.0/24 is directly connected, Vlan1
L      192.168.1.1/32 is directly connected, Vlan1      192.168.2.0/24 is
variably subnetted, 2 subnets, 2 masks
C      192.168.2.0/24 is directly connected, Vlan2
L      192.168.2.1/32 is directly connected, Vlan2
```

- d. Vea la información de la tabla de routing para el R1.

R1# show ip route

*Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override*

Gateway of last resort is not set

```
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.1.0/24 is directly connected, GigabitEthernet0/1
L      192.168.1.10/32 is directly connected, GigabitEthernet0/1
S      192.168.2.0/24 is directly connected, GigabitEthernet0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C      209.165.200.0/27 is directly connected, Loopback0
L      209.165.200.225/32 is directly connected, Loopback0
```

¿Cómo está representada la ruta estática?

S 192.168.2.0/24 está conectada directamente, GigabitEthernet0/1

- e. ¿Es posible hacer ping de la PC-A al R1? _____ **SI**



UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



¿Es posible hacer ping de la PC-A a la interfaz Lo0? _____ **SI**

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

Reflexión

1. Al configurar DHCPv4, ¿por qué excluiría las direcciones estáticas antes de configurar el pool de DHCPv4?

Excluimos las que no se usan y luego dejamos que asigne las demás

2. Si hay varios pools de DHCPv4 presentes, ¿cómo asigna el switch la información de IP a los hosts?

El switch asigna las configuraciones IP según la asignación que haga la VLAN .

3. Además del switching, ¿qué funciones puede llevar a cabo el switch Cisco 2960?

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



El switch puede funcionar como un servidor de DHCP y puede hacer routing estático, realiza también de Router , es una característica mas .

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet n.º 2	Interfaz serial #1	Interfaz serial n.º 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.				

Laboratorio 10.2.3.5 configuración de dhcpv6 sin estado y con estado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Topología

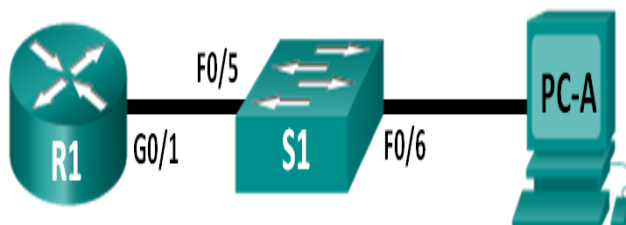


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv6	Longitud de prefijo	Gateway predeterminado
R1	G0/1	2001:DB8:ACAD:A::1	64	No aplicable
S1	VLAN 1	Asignada mediante SLAAC	64	Asignada mediante SLAAC
PC-A	NIC	Asignada mediante SLAAC y DHCPv6	64	Asignado por el R1

Objetivos

- Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
- Parte 2: configurar la red para SLAAC
- Parte 3: configurar la red para DHCPv6 sin estado
- Parte 4: configurar la red para DHCPv6 con estado

Información básica/situación

La asignación dinámica de direcciones IPv6 de unidifusión global se puede configurar de tres maneras:

SOLO MEDIANTE CONFIGURACIÓN AUTOMÁTICA DE DIRECCIÓN SIN ESTADO (SLAAC)

MEDIANTE EL PROTOCOLO DE CONFIGURACIÓN DINÁMICA DE HOST SIN ESTADO PARA IPV6 (DHCPV6)

MEDIANTE DHCPV6 CON ESTADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Con SLAAC (se pronuncia “slac”), no se necesita un servidor de DHCPv6 para que los hosts adquieran direcciones IPv6. Se puede usar para recibir información adicional que necesita el host, como el nombre de dominio y la dirección del servidor de nombres de dominio (DNS). El uso de SLAAC para asignar direcciones host IPv6 y de DHCPv6 para asignar otros parámetros de red se denomina “DHCPv6 sin estado”.

Con DHCPv6 con estado, el servidor de DHCP asigna toda la información, incluida la dirección host IPv6.

La determinación de cómo los hosts obtienen la información de direccionamiento dinámico IPv6 depende de la configuración de indicadores incluida en los mensajes de anuncio de router (RA).

En esta práctica de laboratorio, primero configurará la red para que utilice SLAAC. Una vez que verificó la conectividad, configurará los parámetros de DHCPv6 y modificará la red para que utilice DHCPv6 sin estado. Una vez que verificó que DHCPv6 sin estado funcione correctamente, modificará la configuración del R1 para que utilice DHCPv6 con estado. Se usará Wireshark en la PC-A para verificar las tres configuraciones dinámicas de red.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que el router y el switch se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Nota: la plantilla default bias que utiliza el Switch Database Manager (SDM) no proporciona capacidades de dirección IPv6. Verifique que se utilice la plantilla dual-ipv4-and-ipv6 o la plantilla lanbase-routing en SDM. La nueva plantilla se utilizará después de reiniciar, aunque no se guarde la configuración.

S1# show sdm prefer

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Siga estos pasos para asignar la plantilla dual-ipv4-and-ipv6 como la plantilla de SDM predeterminada:

```
S1# config t
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
S1(config)# end
S1# reload
```

Recursos necesarios

- 1 ROUTER (CISCO 1941 CON IOS DE CISCO VERSIÓN 15.2(4)M3, IMAGEN UNIVERSAL O SIMILAR)**
- 1 SWITCH (CISCO 2960 CON IOS DE CISCO VERSIÓN 15.0(2), IMAGEN LANBASEK9 O COMPARABLE)**
- 1 COMPUTADORA (WINDOWS 7 O VISTA CON WIRESHARK Y UN PROGRAMA DE EMULACIÓN DE TERMINAL, COMO TERA TERM)**
- CABLES DE CONSOLA PARA CONFIGURAR LOS DISPOSITIVOS CON IOS DE CISCO MEDIANTE LOS PUERTOS DE CONSOLA**
- CABLES ETHERNET, COMO SE MUESTRA EN LA TOPOLOGÍA**

Nota: los servicios de cliente DHCPv6 están deshabilitados en Windows XP. Se recomienda usar un host con Windows 7 para esta práctica de laboratorio.

Parte 9. armar la red y configurar los parámetros básicos de los dispositivos

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos de configuración, como los nombres de dispositivos, las contraseñas y las direcciones IP de interfaz.

Paso 1. realizar el cableado de red tal como se muestra en la topología.

Paso 2. inicializar y volver a cargar el router y el switch según sea necesario.

Paso 3. Configurar R1

- a. Desactive la búsqueda del DNS.
- b. Configure el nombre del dispositivo.
- c. Cifre las contraseñas de texto no cifrado.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



- d. Cree un mensaje MOTD que advierta a los usuarios que se prohíbe el acceso no autorizado.
- e. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- f. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.
- g. Establezca el inicio de sesión de consola en modo síncronico.
- h. Guardar la configuración en ejecución en la configuración de inicio.

Paso 4. configurar el S1.

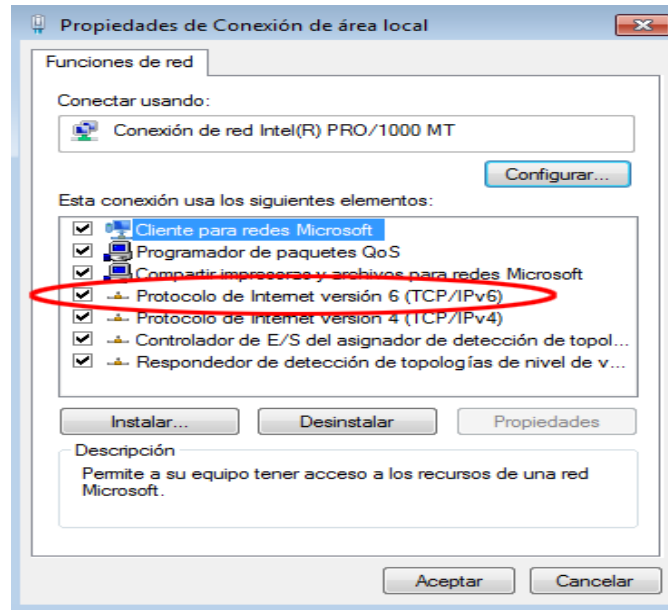
- a. Desactive la búsqueda del DNS.
- b. Configure el nombre del dispositivo.
- c. Cifre las contraseñas de texto no cifrado.
- d. Cree un mensaje MOTD que advierta a los usuarios que se prohíbe el acceso no autorizado.
- e. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- f. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.
- g. Establezca el inicio de sesión de consola en modo síncronico.
- h. Desactive administrativamente todas las interfaces inactivas.
- i. Guarde la configuración en ejecución en la configuración de inicio.

Parte 10. configurar la red para SLAAC

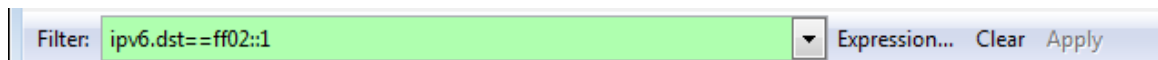
Paso 1. preparar la PC-A.

- a. Verifique que se haya habilitado el protocolo IPv6 en la ventana Propiedades de conexión de área local. Si la casilla de verificación Protocolo de Internet versión 6 (TCP/IPv6) no está marcada, haga clic para activarla.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



- b. Inicie una captura del tráfico en la NIC con Wireshark.
- c. Filtre la captura de datos para ver solo los mensajes RA. Esto se puede realizar mediante el filtrado de paquetes IPv6 con una dirección de destino FF02::1, que es la dirección de solo unidifusión del grupo de clientes. La entrada de filtro que se usa con Wireshark es **ipv6.dst==ff02::1**, como se muestra aquí.



Paso 2. Configurar R1

- a. Habilite el routing de unidifusión IPv6.
- b. Asigne la dirección IPv6 de unidifusión a la interfaz G0/1 según la tabla de direccionamiento.
- c. Asigne FE80::1 como la dirección IPv6 link-local para la interfaz G0/1.
- d. Active la interfaz G0/1.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Paso 3. verificar que el R1 forme parte del grupo de multidifusión de todos los routers.

Use el comando `show ipv6 interface g0/1` **para verificar que G0/1 forme parte del grupo de multidifusión de todos los routers (FF02::2). Los mensajes RA no se envían por G0/1 sin esa asignación de grupo.**

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
```

Paso 4. configurar el S1.

Use el comando `ipv6 address autoconfig` **en la VLAN 1 para obtener una dirección IPv6 a través de SLAAC.**

```
S1(config)# interface vlan 1
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
S1(config-if)# ipv6 address autoconfig
S1(config-if)# end
```

Paso 5. verificar que SLAAC haya proporcionado una dirección de unidifusión al S1.

Use el comando show ipv6 interface para verificar que SLAAC haya proporcionado una dirección de unidifusión a la VLAN1 en el S1.

```
S1# show ipv6 interface
```

Vlan1 is up, line protocol is up

IPv6 is enabled, link-local address is FE80::ED9:96FF:FEE8:8A40

No Virtual link-local address(es):

Stateless address autoconfig enabled

Global unicast address(es):

2001:DB8:ACAD:A:ED9:96FF:FEE8:8A40, subnet is 2001:DB8:ACAD:A::/64
[EUI/CAL/PRE]

valid lifetime 2591988 preferred lifetime 604788

Joined group address(es):

FF02::1

FF02::1:FFE8:8A40

MTU is 1500 bytes

ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled

ICMP unreachable are sent

Output features: Check hwidb

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds (using 30000)

ND NS retransmit interval is 1000 milliseconds

Default router is FE80::1 on Vlan1

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Paso 6. verificar que SLAAC haya proporcionado información de dirección IPv6 en la PC-A.

- En el símbolo del sistema de la PC-A, emita el comando **ipconfig /all**. Verifique que la PC-A muestre una dirección IPv6 con el prefijo 2001:db8:acad:a::/64. El gateway predeterminado debe tener la dirección FE80::1.

```
Adaptador de Ethernet Conexión de área local:
    Sufijo DNS específico para la conexión. . . : 
    Descripción . . . . . : Conexión de red Intel(R) PRO/1000
    MT
    Dirección física. . . . . : 00-0C-29-E3-23-17
    DHCP habilitado . . . . . : sí
    Configuración automática habilitada . . . : sí
    Dirección IPv6 . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88<Preferido>
    Vínculo: dirección IPv6 local. . . : fe80::e8ed:811c:3215:5bc2%11<Preferido>

    Dirección IPv4. . . . . : 192.168.96.139<Preferido>
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . : fe80::1%11
    Servidores DNS . . . . . : fec0:0:0:ffff::1%1
                                fec0:0:0:ffff::2%1
                                fec0:0:0:ffff::3%1
    NetBIOS sobre TCP/IP. . . . . : habilitado
```

- En Wireshark, observe uno de los mensajes RA que se capturaron. Expanda la capa Internet Control Message Protocol v6 (Protocolo de mensajes de control de Internet v6) para ver la información de Flags (Indicadores) y Prefix (Prefijo). Los primeros dos indicadores controlan el uso de DHCPv6 y no se establecen si no se configura DHCPv6. La información del prefijo también está incluida en este mensaje RA.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Filter: **ipv6.dst==ff02::1** Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
3518	3972.07973	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1
3673	4130.43155	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1
3840	4284.68370	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1
3989	4435.87602	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1

Frame 3518: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)

Ethernet II, Src: d4:8c:b5:ce:a0:c1 (d4:8c:b5:ce:a0:c1), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)

Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: ff02::1 (ff02::1)

Internet Control Message Protocol v6

Type: Router Advertisement (134)

Code: 0

Checksum: 0x1816 [correct]

Cur hop limit: 64

Flags: 0x00

0... .. = Managed address configuration: Not set

.0... .. = Other configuration: Not set

..0... .. = Home Agent: Not set

...0 0... = Prf (Default Router Preference): Medium (0)

.... 0... = Proxy: Not set

.... ..0. = Reserved: 0

Router lifetime (s): 1800

Reachable time (ms): 0

Retrans timer (ms): 0

ICMPv6 option (Source link-layer address : d4:8c:b5:ce:a0:c1)

ICMPv6 option (MTU : 1500)

ICMPv6 option (Prefix information : 2001:db8:acad:a::/64)

Type: Prefix information (3)

Length: 4 (32 bytes)

Prefix Length: 64

Flag: 0xc0

Valid Lifetime: 2592000

Preferred Lifetime: 604800

Reserved

Prefix: 2001:db8:acad:a:: (2001:db8:acad:a::)

Parte 11. configurar la red para DHCPv6 sin estado

Paso 1. configurar un servidor de DHCP IPv6 en el R1.

- Cree un pool de DHCP IPv6.
R1(config)# **ipv6 dhcp pool IPV6POOL-A**
- Asigne un nombre de dominio al pool.
R1(config-dhcpv6)# **domain-name ccna-statelessDHCPv6.com**
- Asigne una dirección de servidor DNS.
R1(config-dhcpv6)# **dns-server 2001:db8:acad:a::abcd**
R1(config-dhcpv6)# **exit**
- Asigne el pool de DHCPv6 a la interfaz.
R1(config)# **interface g0/1**
R1(config-if)# **ipv6 dhcp server IPV6POOL-A**
- Establezca la detección de redes (ND) DHCPv6 **other-config-flag**.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
R1(config-if)# ipv6 nd other-config-flag  
R1(config-if)# end
```

Paso 2. verificar la configuración de DHCPv6 en la interfaz G0/1 del R1.

Use el comando show ipv6 interface g0/1 para verificar que la interfaz ahora forme parte del grupo IPv6 de multidifusión de todos los servidores de DHCPv6 (FF02::1:2). La última línea del resultado de este comando show verifica que se haya establecido other-config-flag.

```
R1# show ipv6 interface g0/1  
GigabitEthernet0/1 is up, line protocol is up  
IPv6 is enabled, link-local address is FE80::1  
No Virtual link-local address(es):  
Global unicast address(es):  
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64  
Joined group address(es):  
  FF02::1  
  FF02::2  
  FF02::1:2  
  FF02::1:FF00:1  
  FF05::1:3  
MTU is 1500 bytes  
ICMP error messages limited to one every 100 milliseconds  
ICMP redirects are enabled  
ICMP unreachable are sent  
ND DAD is enabled, number of DAD attempts: 1  
ND reachable time is 30000 milliseconds (using 30000)  
ND advertised reachable time is 0 (unspecified)  
ND advertised retransmit interval is 0 (unspecified)  
ND router advertisements are sent every 200 seconds  
ND router advertisements live for 1800 seconds  
ND advertised default router preference is Medium  
Hosts use stateless autoconfig for addresses.
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Hosts use DHCP to obtain other configuration.

Paso 3. ver los cambios realizados en la red en la PC-A.

Use el comando `ipconfig /all` para revisar los cambios realizados en la red. Observe que se recuperó información adicional, como la información del nombre de dominio y del servidor DNS, del servidor de DHCPv6. Sin embargo, las direcciones IPv6 de unidifusión global y link-local se obtuvieron previamente mediante SLAAC.

```
Adaptador de Ethernet Conexión de área local:
Sufijo DNS específico para la conexión. . . : ccna-statelessDHCPv6.com
Descripción . . . . . : Conexión de red Intel(R) PRO/1000
MT
Dirección física. . . . . : 00-0C-29-E3-23-17
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Dirección IPv6 . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88<Preferido>
Vínculo: dirección IPv6 local. . . : fe80::e8ed:811c:3215:5bc2%11<Preferido>
Dirección IPv4. . . . . : 192.168.96.139<Preferido>
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . : fe80::1%11
IAID DHCPv6 . . . . . : 234884137
DUID de cliente DHCPv6. . . . . : 00-01-00-01-19-A7-DD-BE-00-0C-29-E3-23-17
Servidores DNS. . . . . : 2001:db8:acad:a::abcd
NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de túnel isatap.localdomain:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . : ccna-statelessDHCPv6.com
Descripción . . . . . : Adaptador ISATAP de Microsoft
Dirección física. . . . . : 00-00-00-00-00-00-00-E0
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí
```

Paso 4. ver los mensajes RA en Wireshark.

Desplácese hasta el último mensaje RA que se muestra en Wireshark y expándalo para ver la configuración de indicadores ICMPv6. Observe que el indicador Other configuration (Otra configuración) está establecido en 1.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



No.	Time	Source	Destination	Protocol	Length	Info
191	190.005980	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1
422	383.803033	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1
696	581.355847	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1
877	776.644829	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1

Frame 877: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)	
Ethernet II, Src: d4:8c:b5:ce:a0:c1 (d4:8c:b5:ce:a0:c1), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)	
Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: ff02::1 (ff02::1)	
Internet Control Message Protocol v6	
Type: Router Advertisement (134)	
Code: 0	
Checksum: 0x17d6 [correct]	
Cur hop limit: 64	
Flags: 0x40	
0... .. = Managed address configuration: Not set	
.1... .. = Other configuration: Set	
..0... .. = Home Agent: Not set	
...0... = Prf (Default Router Preference): Medium (0)	
....0... = Proxy: Not set	
.....0... = Reserved: 0	
Router lifetime (s): 1800	
Reachable time (ms): 0	
Retrans timer (ms): 0	
ICMPv6 Option (Source link-layer address : d4:8c:b5:ce:a0:c1)	
ICMPv6 Option (MTU : 1500)	
ICMPv6 Option (Prefix information : 2001:db8:acad:a::/64)	

Paso 5. verificar que la PC-A no haya obtenido su dirección IPv6 de un servidor de DHCPv6.

Use los comandos **show ipv6 dhcp binding** y **show ipv6 dhcp pool** para verificar que la PC-A no haya obtenido una dirección IPv6 del pool de DHCPv6.

```
R1# show ipv6 dhcp binding
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
DNS server: 2001:DB8:ACAD:A::ABCD
Domain name: ccna-statelessDHCPv6.com
Active clients: 0
```

Paso 6. restablecer la configuración de red IPv6 de la PC-A.

- Desactive la interfaz F0/6 del S1.

Nota: la desactivación de la interfaz F0/6 evita que la PC-A reciba una nueva dirección IPv6 antes de que usted vuelva a configurar el R1 para DHCPv6 con estado en la parte 4.

```
S1(config)# interface f0/6
S1(config-if)# shutdown
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



- b. Detenga la captura de tráfico con Wireshark en la NIC de la PC-A.
- c. Restablezca la configuración de IPv6 en la PC-A para eliminar la configuración de DHCPv6 sin estado.
 - 1) Abra la ventana Propiedades de conexión de área local, desactive la casilla de verificación **Protocolo de Internet versión 6 (TCP/IPv6)** y haga clic en **Aceptar** para aceptar el cambio.
 - 2) Vuelva a abrir la ventana Propiedades de conexión de área local, haga clic para habilitar la casilla de verificación **Protocolo de Internet versión 6 (TCP/IPv6)** y, a continuación, haga clic en **Aceptar** para aceptar el cambio.

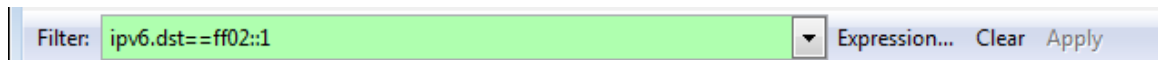
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Parte 12. configurar la red para DHCPv6 con estado

Paso 1. preparar la PC-A.

- Inicie una captura del tráfico en la NIC con Wireshark.
- Filtre la captura de datos para ver solo los mensajes RA. Esto se puede realizar mediante el filtrado de paquetes IPv6 con una dirección de destino FF02::1, que es la dirección de solo unidifusión del grupo de clientes.



Paso 2. cambiar el pool de DHCPv6 en el R1.

- Agregue el prefijo de red al pool.

```
R1(config)# ipv6 dhcp pool IPV6POOL-A  
R1(config-dhcpv6)# address prefix 2001:db8:acad:a::/64
```
- Cambie el nombre de dominio a **ccna-statefulDHCPv6.com**.
Nota: debe eliminar el antiguo nombre de dominio. El comando **domain-name** no lo reemplaza.

```
R1(config-dhcpv6)# no domain-name ccna-statelessDHCPv6.com  
R1(config-dhcpv6)# domain-name ccna-StatefulDHCPv6.com  
R1(config-dhcpv6)# end
```

- Verifique la configuración del pool de DHCPv6.

```
R1# show ipv6 dhcp pool  
DHCPv6 pool: IPV6POOL-A  
Address allocation prefix: 2001:DB8:ACAD:A::/64 valid 172800 preferred 86400  
(0 in use, 0 conflicts)  
DNS server: 2001:DB8:ACAD:A::ABCD  
Domain name: ccna-StatefulDHCPv6.com  
Active clients: 0
```
- Ingrese al modo de depuración para verificar la asignación de direcciones de DHCPv6 con estado.

```
R1# debug ipv6 dhcp detail
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



IPv6 DHCP debugging is on (detailed)

Paso 3. establecer el indicador en G0/1 para DHCPv6 con estado.

Nota: la desactivación de la interfaz G0/1 antes de realizar cambios asegura que se envíe un mensaje RA cuando se activa la interfaz.

```
R1(config)# interface g0/1
R1(config-if)# shutdown
R1(config-if)# ipv6 nd managed-config-flag
R1(config-if)# no shutdown
R1(config-if)# end
```

habilitar la interfaz F0/6 en el S1.

Ahora que configuró el R1 para DHCPv6 con estado, puede volver a conectar la PC-A a la red activando la interfaz F0/6 en el S1.

```
S1(config)# interface f0/6
S1(config-if)# no shutdown
S1(config-if)# end
```

Paso 4. verificar la configuración de DHCPv6 con estado en el R1.

- Emita el comando **show ipv6 interface g0/1** para verificar que la interfaz esté en el modo DHCPv6 con estado.

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:2
  FF02::1:FF00:1
  FF05::1:3
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use DHCP to obtain routable addresses.
Hosts use DHCP to obtain other configuration.

- b. En el símbolo del sistema de la PC-A, escriba **ipconfig /release6** para liberar la dirección IPv6 asignada actualmente. Luego, escriba **ipconfig /renew6** para solicitar una dirección IPv6 del servidor de DHCPv6.
- c. Emita el comando **show ipv6 dhcp pool** para verificar el número de clientes activos.

R1# **show ipv6 dhcp pool**

DHCPv6 pool: IPV6POOL-A

Address allocation prefix: 2001:DB8:ACAD:A::/64 valid 172800 preferred 86400
(1 in use, 0 conflicts)

DNS server: 2001:DB8:ACAD:A::ABCD

Domain name: ccna-StatefulDHCPv6.com

Active clients: 1

- d. Emita el comando **show ipv6 dhcp binding** para verificar que la PC-A haya recibido su dirección IPv6 de unidifusión del pool de DHCP. Compare la dirección de cliente con la dirección IPv6 link-local en la PC-A mediante el comando **ipconfig /all**. Compare la dirección proporcionada por el comando **show** con la dirección IPv6 que se indica con el comando **ipconfig /all** en la PC-A.

R1# **show ipv6 dhcp binding**

Client: FE80::D428:7DE2:997C:B05A

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



DUID: 0001000117F6723D000C298D5444
Username : unassigned
IA NA: IA ID 0x0E000C29, T1 43200, T2 69120
Address: 2001:DB8:ACAD:A:B55C:8519:8915:57CE
preferred lifetime 86400, valid lifetime 172800
expires at Mar 07 2013 04:09 PM (171595 seconds)

```
Adaptador de Ethernet Conexión de área local:
  Sufijo DNS específico para la conexión. . : ccna-StatefulDHCPv6.com
  Descripción . . . . . : Conexión de red Intel(R) PRO/1000
MT
  Dirección física. . . . . : 00-0C-29-E3-23-17
  DHCP habilitado . . . . . : sí
  Configuración automática habilitada . . . : sí
  Dirección IPv6 . . . . . : 2001:db8:acad:a:b55c:8519:8915:57ce<Preferido>
  Concesión obtenida. . . . . : jueves, 05 de septiembre de 2013
16:07:59
  La concesión expira . . . . . : jueves, 05 de septiembre de 2013
16:38:03
  Dirección IPv6 . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88<Preferido>
  Vínculo: dirección IPv6 local. . . : fe80::d428:7de2:997c:b05a%11<Preferido>
  Dirección IPv4. . . . . : 192.168.96.139<Preferido>
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . : fe80::1%11
  IAID DHCPv6 . . . . . : 234884137
  DUID de cliente DHCPv6. . . . . : 00-01-00-01-19-A7-DD-BE-00-0C-29-E3-23-17
  Servidores DNS . . . . . : 2001:db8:acad:a::abcd
  NetBIOS sobre TCP/IP. . . . . : habilitado
```

- e. Emita el comando **undebg all** en el R1 para detener la depuración de DHCPv6.

Nota: escribir **u all** es la forma más abreviada de este comando y sirve para saber si quiere evitar que los mensajes de depuración se desplacen hacia abajo constantemente en la pantalla de la sesión de terminal. Si hay varias depuraciones en proceso, el comando **undebg all** las detiene todas.

R1# **u all**

Se ha desactivado toda depuración posible

- f. Revise los mensajes de depuración que aparecieron en la pantalla de terminal del R1.

1) Examine el mensaje de solicitud de la PC-A que solicita información de red.

*Mar 5 16:42:39.775: IPv6 DHCP: Received SOLICIT from
FE80::D428:7DE2:997C:B05A on GigabitEthernet0/1

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
*Mar 5 16:42:39.775: IPv6 DHCP: detailed packet contents
*Mar 5 16:42:39.775: src FE80::D428:7DE2:997C:B05A (GigabitEthernet0/1)
*Mar 5 16:42:39.775: dst FF02::1:2
*Mar 5 16:42:39.775: type SOLICIT(1), xid 1039238
*Mar 5 16:42:39.775: option ELAPSED-TIME(8), len 2
*Mar 5 16:42:39.775: elapsed-time 6300
*Mar 5 16:42:39.775: option CLIENTID(1), len 14

2) Examine el mensaje de respuesta enviado a la PC-A con la información de red
   DHCP.

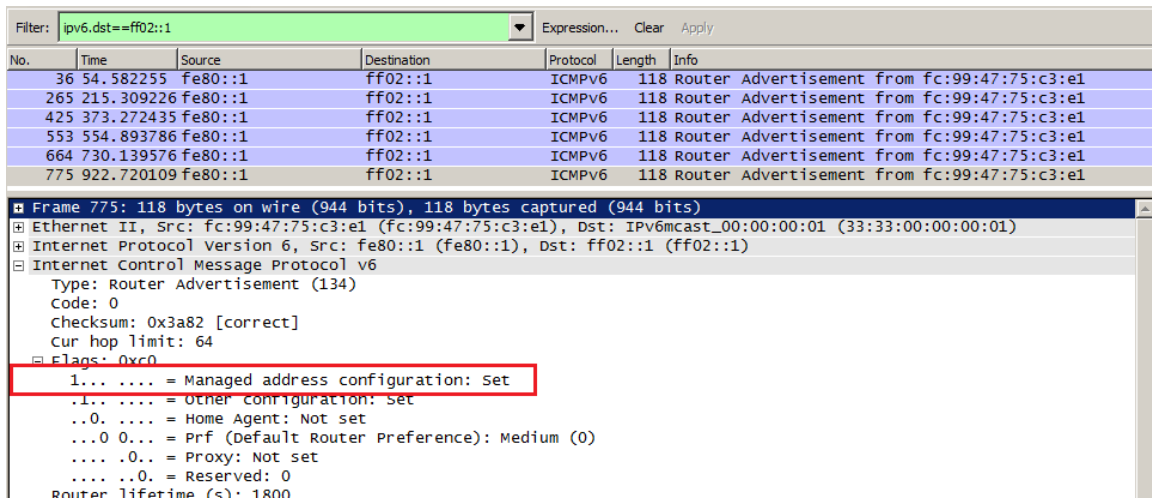
*Mar 5 16:42:39.779: IPv6 DHCP: Sending REPLY to
FE80::D428:7DE2:997C:B05A on GigabitEthernet0/1
*Mar 5 16:42:39.779: IPv6 DHCP: detailed packet contents
*Mar 5 16:42:39.779: src FE80::1
*Mar 5 16:42:39.779: dst FE80::D428:7DE2:997C:B05A (GigabitEthernet0/1)
*Mar 5 16:42:39.779: type REPLY(7), xid 1039238
*Mar 5 16:42:39.779: option SERVERID(2), len 10
*Mar 5 16:42:39.779: 00030001FC994775C3E0
*Mar 5 16:42:39.779: option CLIENTID(1), len 14
*Mar 5 16:42:39.779: 00010001
R1#17F6723D000C298D5444
*Mar 5 16:42:39.779: option IA-NA(3), len 40
*Mar 5 16:42:39.779: IAID 0x0E000C29, T1 43200, T2 69120
*Mar 5 16:42:39.779: option IAADDR(5), len 24
*Mar 5 16:42:39.779: IPv6 address
2001:DB8:ACAD:A:B55C:8519:8915:57CE
*Mar 5 16:42:39.779: preferred 86400, valid 172800
*Mar 5 16:42:39.779: option DNS-SERVERS(23), len 16
*Mar 5 16:42:39.779: 2001:DB8:ACAD:A::ABCD
*Mar 5 16:42:39.779: option DOMAIN-LIST(24), len 26
*Mar 5 16:42:39.779: ccna-StatefulDHCPv6.com
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Paso 5. verificar DHCPv6 con estado en la PC-A.

- Detenga la captura de Wireshark en la PC-A.
- Expanda el mensaje RA más reciente que se indica en Wireshark. Verifique que se haya establecido el indicador **Managed address configuration** (Configuración de dirección administrada).



- Cambie el filtro en Wireshark para ver solo los paquetes **DHCPv6** escribiendo **dhcpv6** y, a continuación, haga clic en **Apply** (Aplicar). Resalte la última respuesta DHCPv6 de la lista y expanda la información de DHCPv6. Examine la información de red DHCPv6 incluida en este paquete.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Filter:	dhcpv6	Expression...	Clear	Apply		
No.	Time	Source	Destination	Protocol	Length	Info
250	443.078236	fe80::d428:7de2:997ff02::1:2		DHCPv6	146	Solicit XID: 0x2b2a8e CID: 0001000117f6723d000c2
267	475.083284	fe80::d428:7de2:997ff02::1:2		DHCPv6	146	Solicit XID: 0x2b2a8e CID: 0001000117f6723d000c2
425	656.281211	fe80::d428:7de2:997ff02::1:2		DHCPv6	146	Solicit XID: 0xc86c32 CID: 0001000117f6723d000c2
429	656.282249	fe80::1	fe80::d428:7de2:997ff02::1:2	DHCPv6	191	Advertise XID: 0xc86c32 CID: 0001000117f6723d000c2
460	657.292018	fe80::d428:7de2:997ff02::1:2		DHCPv6	188	Request XID: 0xc86c32 CID: 0001000117f6723d000c2
462	657.292638	fe80::1	fe80::d428:7de2:997ff02::1:2	DHCPv6	191	Reply XID: 0xc86c32 CID: 0001000117f6723d000c298
Ethernet II, Src: fc:99:47:75:c3:e1 (fc:99:47:75:c3:e1), Dst: Vmware_be:6c:89 (00:50:56:be:6c:89)						
Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: fe80::d428:7de2:997c:b05a (fe80::d428:7de2:997c:b05a)						
User Datagram Protocol, Src Port: dhcpv6-server (547), Dst Port: dhcpv6-client (546)						
DHCPv6						
Message type: Reply (7)						
Transaction ID: 0xc86c32						
Server Identifier: 00030001fc994775c3e0						
Client Identifier: 0001000117f6723d000c298d5444						
Identity Association for Non-temporary Address						
Option: Identity Association for Non-temporary Address (3)						
Length: 40						
Value: 0e000c290000a8c000010e000005001820010db8acad000a...						
IAID: 0e000c29						
T1: 43200						
T2: 69120						
IA Address: 2001:db8:acad:a:b55c:8519:8915:57ce						
DNS recursive name server						
Option: DNS recursive name server (23)						
Length: 16						
Value: 20010db8acad000a000000000000abcd						
DNS servers address: 2001:db8:acad:a::abcd						
Domain Search List						
Option: Domain Search List (24)						
Length: 25						
Value: 1363636e612d537461746566756c44484350763603636f6d...						
DNS Domain Search List						
Domain: ccna-StatefulDHCPv6.com						

Reflexión

- ¿Qué método de direccionamiento IPv6 utiliza más recursos de memoria en el router configurado como servidor de DHCPv6: DHCPv6 sin estado o DHCPv6 con estado? ¿Por qué?:

El protocolo DHCP permite configurar automáticamente los host de una red TCP/IP durante el arranque de los sistemas. DHCP utiliza un mecanismo de cliente-servidor, a la vez los servidores almacenan y gestionan la información de configuración de los clientes y la suministran cuando éstos la solicitan.

DHCPv6 requiere el router para almacenar la información de estado dinámica sobre los clientes DHCPv6, este método de direccionamiento con estado utiliza más recursos de memoria en el router que el método sin estado.

- ¿Qué tipo de asignación dinámica de direcciones IPv6 recomienda Cisco: DHCPv6 sin estado o DHCPv6 con estado?: Cisco recomienda sin estado DHCPv6 en la aplicación.

Se recomienda que los dispositivos ipv6 realicen detección de direcciones duplicadas en cualquier dirección, en la configuración automática de

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



direcciones sin estado se utiliza para configurar las direcciones locales de vínculos y las direcciones no locales de vínculos adicionales mediante el intercambio de mensajes de solicitud de enrutador y anuncio de enrutador con los enrutadores vecinos.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet n.º 2	Interfaz serial #1	Interfaz serial n.º 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

Laboratorio 10.3.1.1 Packet Tracer - IdT y DHCP

Objetivo

Configure DHCP para IPv4 o IPv6 en un router Cisco 1941.

Situación

En este capítulo, se presenta el concepto del uso del proceso de DHCP en la red de una pequeña a mediana empresa; sin embargo, el protocolo DHCP también tiene otros usos. Con la llegada de Internet de todo (IdT), podrá acceder a todos los dispositivos en su hogar que admitan conectividad por cable o inalámbrica a una red desde casi cualquier lugar.

Con Packet Tracer, realice las siguientes tareas para esta actividad de creación de modelos:

CONFIGURE UN ROUTER CISCO 1941 (O UN DISPOSITIVO ISR QUE PUEDA ADMITIR UN SERVIDOR DE DHCP) PARA LAS DIRECCIONES IPV4 O IPV6 DE DHCP.

PIENSE EN CINCO DISPOSITIVOS DE SU HOGAR EN LOS QUE DESEE RECIBIR DIRECCIONES IP DESDE EL SERVICIO DHCP DEL ROUTER. CONFIGURE LAS TERMINALES PARA SOLICITAR DIRECCIONES DHCP DEL SERVIDOR DE DHCP. MUESTRE LOS RESULTADOS QUE VALIDEN QUE CADA TERMINAL GARANTIZA UNA DIRECCIÓN IP DEL SERVIDOR. UTILICE UN PROGRAMA DE CAPTURA DE PANTALLA PARA GUARDAR LA INFORMACIÓN DEL RESULTADO O EMPLEE EL COMANDO DE LA TECLA IMPRPANT.

PRESENTE SUS CONCLUSIONES A UN COMPAÑERO DE CLASE O A LA CLASE.

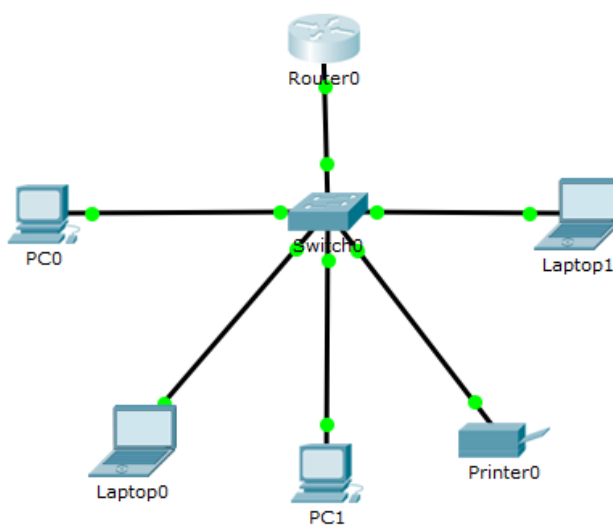
Recursos necesarios

Software de Packet Tracer

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

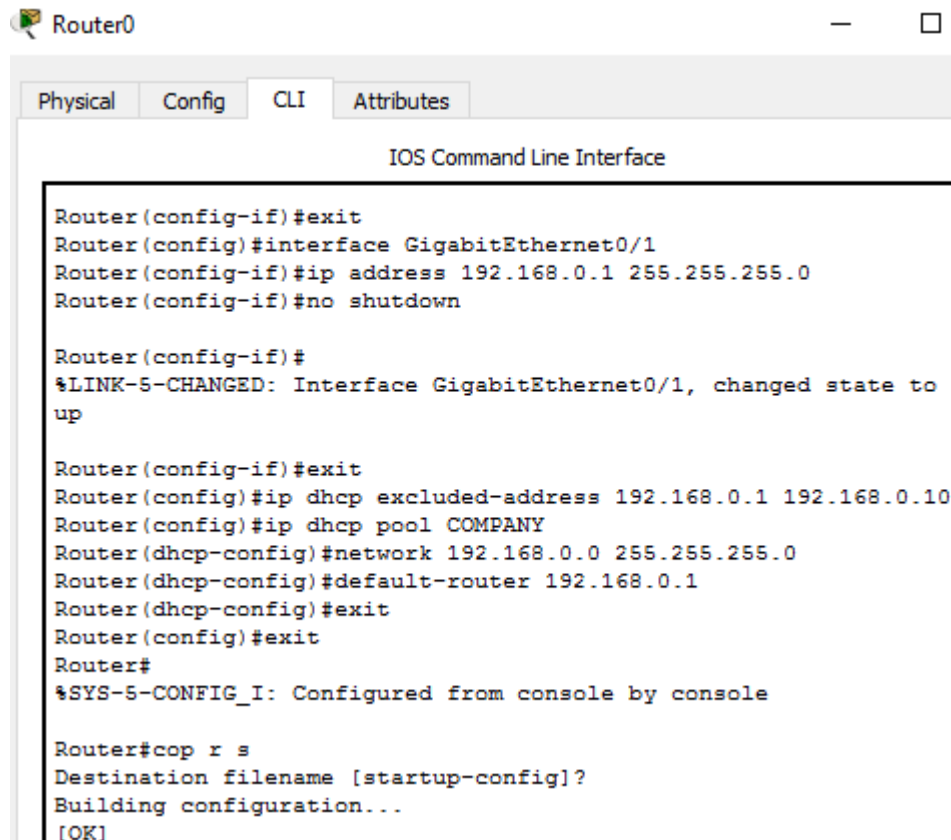


Topología



Configuración del Router:

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```

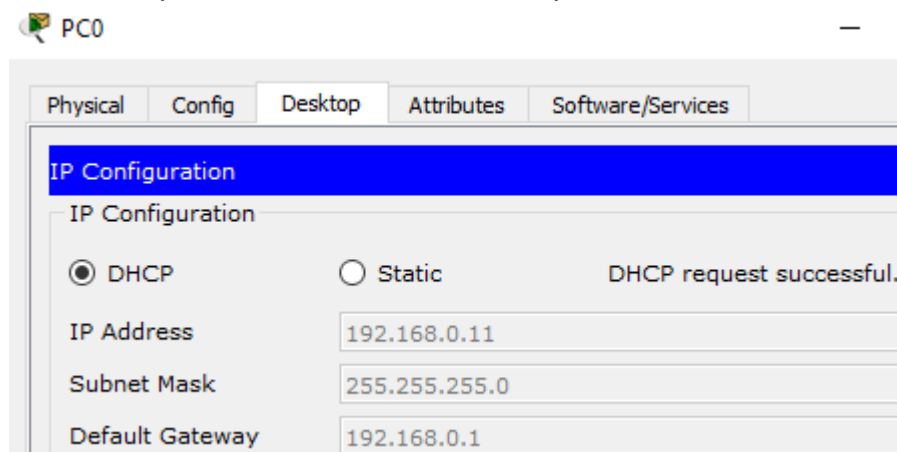
Router0
Router0
Physical Config CLI Attributes
IOS Command Line Interface
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
up

Router(config-if)#exit
Router(config)#ip dhcp excluded-address 192.168.0.1 192.168.0.10
Router(config)#ip dhcp pool COMPANY
Router(dhcp-config)#network 192.168.0.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.0.1
Router(dhcp-config)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
  
```

Asignación automática por servidor DHCP de la IP para el PC0



PC0

Physical Config Desktop Attributes Software/Services

IP Configuration

IP Configuration

☒ DHCP ☐ Static DHCP request successful.

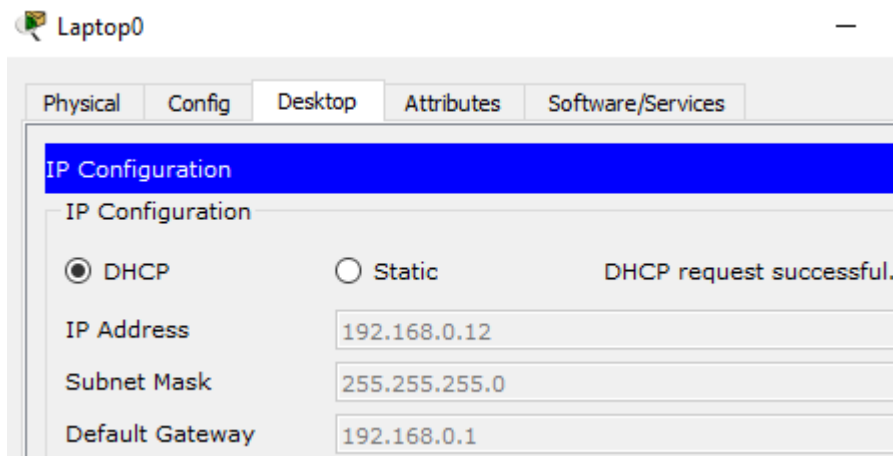
IP Address 192.168.0.11

Subnet Mask 255.255.255.0

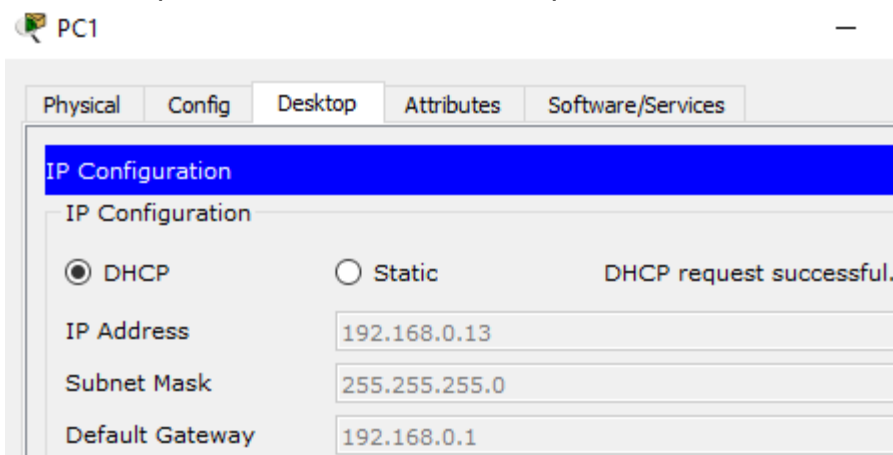
Default Gateway 192.168.0.1

Asignación automática por servidor DHCP de la IP para el Laptop0

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

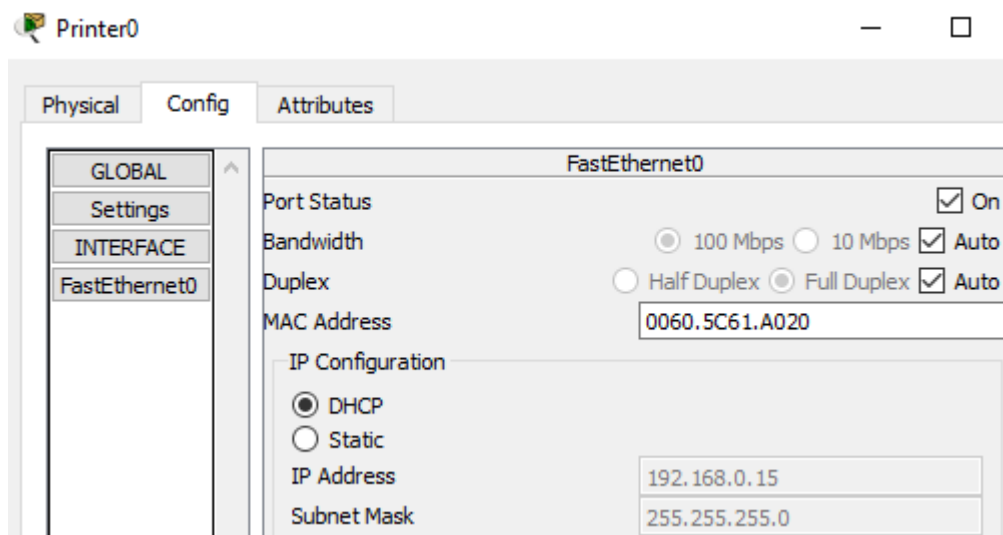


Asignación automática por servidor DHCP de la IP para el PC1

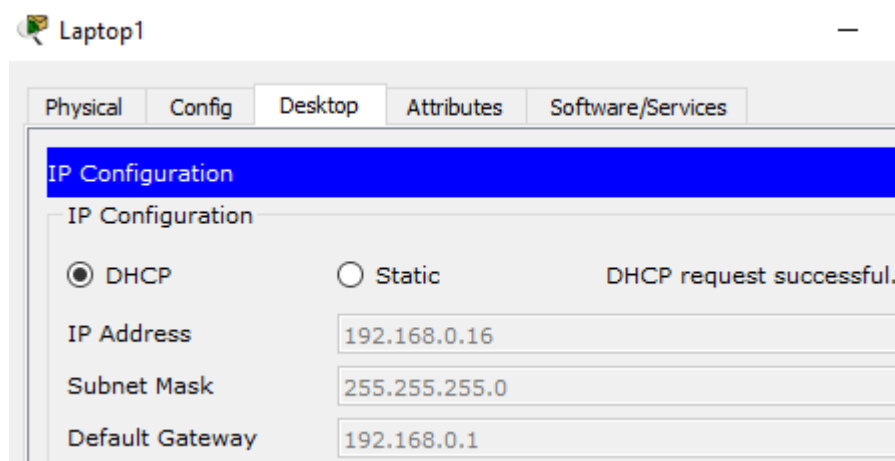


Asignación automática por servidor DHCP de la IP para la Printer0

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

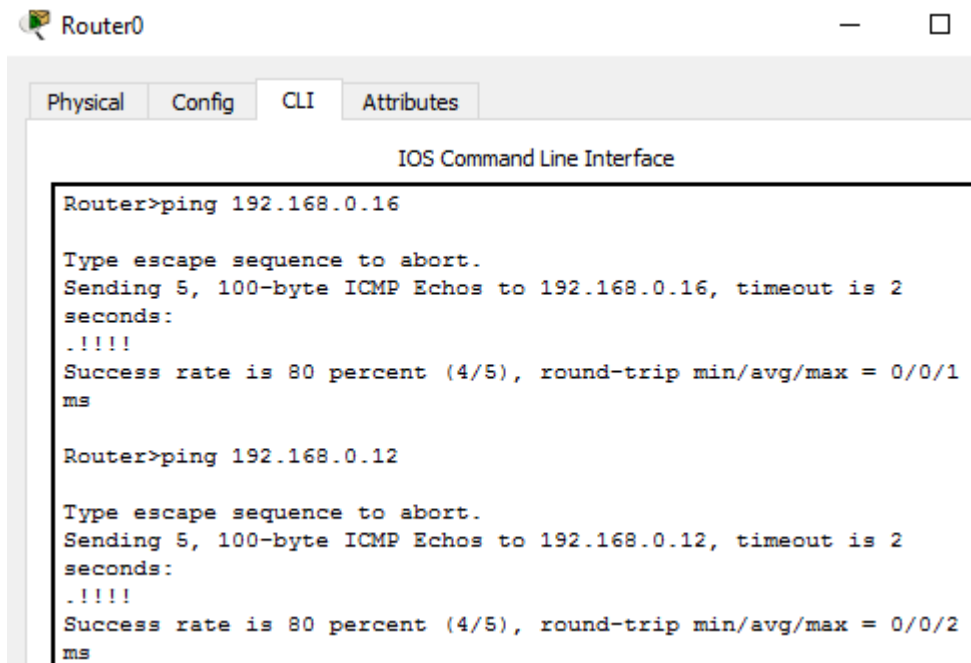


Asignación automática por servidor DHCP de la IP para el Laptop1



UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

Prueba de conectividad entre el Router 0 y laptop 1 y 2:



```
Router0
Physical Config CLI Attributes
IOS Command Line Interface
Router>ping 192.168.0.16
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.16, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1
ms

Router>ping 192.168.0.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.12, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/2
ms
```

Prueba de conectividad entre el PC0 y Printer0:

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

PC0

```

Physical Config Desktop Attributes Software/Services
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.15

Pinging 192.168.0.15 with 32 bytes of data:

Reply from 192.168.0.15: bytes=32 time=1ms TTL=128
Reply from 192.168.0.15: bytes=32 time<1ms TTL=128
Reply from 192.168.0.15: bytes=32 time<1ms TTL=128
Reply from 192.168.0.15: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

```

Prueba de conectividad entre el PC1 y Router0:

PC1

```

Physical Config Desktop Attributes Software/Services
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Reflexión

1. **¿Por qué un usuario desearía usar un router Cisco 1941 para configurar DHCP en su red doméstica? ¿No sería suficiente usar un ISR más pequeño como servidor de DHCP?**

R/ Por su bajo costo y fácil configuración. No se necesita Robustez.

2. **¿Cómo cree que las pequeñas y medianas empresas pueden usar la asignación de direcciones IP de DHCP en el mundo de las redes IPv6 e IdT? Mediante la técnica de la lluvia de ideas, piense y registre cinco respuestas posibles.**

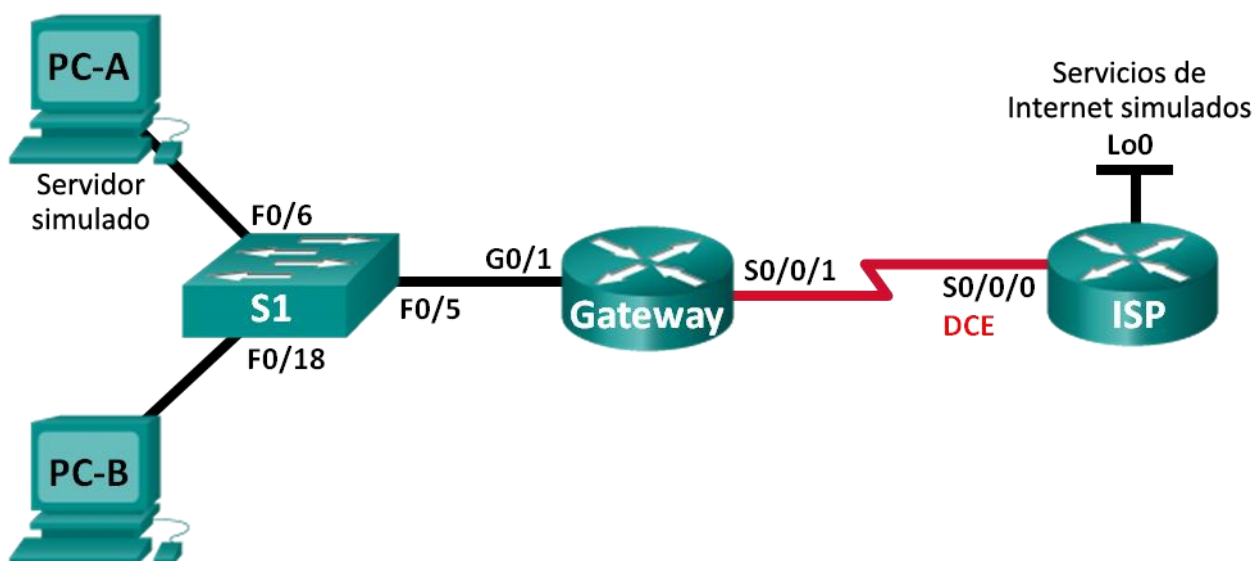
- ✓ IPv6 tiene más capacidad de direccionamiento lo que permite escalar la red.
- ✓ IPv6 es extremadamente dinámico lo cual lo hace muy fácil de configurar.
- ✓ La seguridad que se puede crear en IPv6 es mucho más alta que la que se puede configurar en un router básico.
- ✓ IPV6 puede conectar multiples dispositivos entre ellos celulares, sistemas operativos, y diferentes equipos.
- ✓ IPV6 puede gestionar mejor los recursos y así dar unas conexiones mucho más rápidas a internet por ejemplo.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Laboratorio 11.2.2.6 configuración de NAT dinámica y estática

Topología



UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	G0/0	192.31.7.1	255.255.255.0	N/A
Server ISP	NIC	192.31.7.2	255.255.255.0	192.31.7.1
PC-A (servidor simulado)	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1

Objetivos

Parte 1: armar la red y verificar la conectividad

Parte 2: configurar y verificar la NAT estática

Parte 3: configurar y verificar la NAT dinámica

Información básica/situación

La traducción de direcciones de red (NAT) es el proceso en el que un dispositivo de red, como un router Cisco, asigna una dirección pública a los dispositivos host dentro de una red privada. El motivo principal para usar NAT es reducir el número de direcciones IP públicas que usa una organización, ya que la cantidad de direcciones IPv4 públicas disponibles es limitada.

En esta práctica de laboratorio, un ISP asignó a una empresa el espacio de direcciones IP públicas 209.165.200.224/27. Esto proporciona 30 direcciones IP públicas a la empresa. Las direcciones 209.165.200.225 a 209.165.200.241 son para la asignación estática, y las direcciones 209.165.200.242 a 209.165.200.254 son para la asignación dinámica. Del ISP al router de gateway se usa una ruta

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



estática, y del gateway al router ISP se usa una ruta predeterminada. La conexión del ISP a Internet se simula mediante una dirección de loopback en el router ISP.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y el switch se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios

2 ROUTERS (CISCO 1941 CON IOS DE CISCO VERSIÓN 15.2(4)M3, IMAGEN UNIVERSAL O SIMILAR)

1 SWITCH (CISCO 2960 CON IOS DE CISCO VERSIÓN 15.0(2), IMAGEN LANBASEK9 O COMPARABLE)

2 COMPUTADORAS (WINDOWS 7, VISTA O XP CON UN PROGRAMA DE EMULACIÓN DE TERMINAL, COMO TERA TERM)

CABLES DE CONSOLA PARA CONFIGURAR LOS DISPOSITIVOS CON IOS DE CISCO MEDIANTE LOS PUERTOS DE CONSOLA

CABLES ETHERNET Y SERIALES, COMO SE MUESTRA EN LA TOPOLOGÍA

Parte 13. armar la red y verificar la conectividad

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de interfaz, el routing estático, el acceso a los dispositivos y las contraseñas.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Paso 1. realizar el cableado de red tal como se muestra en la topología.

Conecte los dispositivos tal como se muestra en el diagrama de la topología y realice el cableado según sea necesario.

Paso 2. configurar los equipos host.

Paso 3. inicializar y volver a cargar los routers y los switches según sea necesario.

Paso 4. configurar los parámetros básicos para cada router.

- Desactive la búsqueda del DNS.
- Configure las direcciones IP para los routers como se indica en la tabla de direccionamiento.
- Establezca la frecuencia de reloj en **1280000** para las interfaces seriales DCE.
- Configure el nombre del dispositivo como se muestra en la topología.
- Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- Configure **logging synchronous** para evitar que los mensajes de consola interrumpen la entrada del comando.

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Gateway
Gateway(config)#username cisco pass
Gateway(config)#username cisco password cisco
Gateway(config)#line console 0
Gateway(config-line)#login local
Gateway(config-line)#logging syn
Gateway(config-line)#logging synchronous
Gateway(config-line)#exit
Gateway(config)#no ip domain-lo
Gateway(config)#no ip domain-lookup
Gateway(config)#enable secret class
Gateway(config)#line vty 0 4
Gateway(config-line)#login local
Gateway(config-line)#logging synchronous
Gateway(config-line)#exit
```


UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Paso 5. crear un servidor web simulado en el ISP.

- Cree un usuario local denominado **webuser** con la contraseña cifrada **webpass**.
ISP(config)# **username webuser privilege 15 secret webpass**
- Habilite el servicio del servidor HTTP en el ISP.
ISP(config)# **ip http server**
- Configure el servicio HTTP para utilizar la base de datos local.
ISP(config)# **ip http authentication local**

Paso 6. configurar el routing estático.

- Cree una ruta estática del router ISP al router Gateway usando el rango asignado de direcciones de red públicas 209.165.200.224/27.
ISP(config)# **ip route 209.165.200.224 255.255.255.224 209.165.201.18**
- Cree una ruta predeterminada del router Gateway al router ISP.
Gateway(config)# **ip route 0.0.0.0 0.0.0.0 209.165.201.17**

Paso 7. Guardar la configuración en ejecución en la configuración de inicio.

Paso 8. Verificar la conectividad de la red

- Desde los equipos host, haga ping a la interfaz G0/1 en el router Gateway. Resuelva los problemas si los pings fallan.

```
Packet Tracer SERVER Command Line 1.0
SERVER>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=54ms TTL=255
Reply from 192.168.1.1: bytes=32 time=2ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=21ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 54ms, Average = 19ms
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=18ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=13ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 18ms, Average = 7ms
```

- b. Muestre las tablas de routing en ambos routers para verificar que las rutas estáticas se encuentren en la tabla de routing y estén configuradas correctamente en ambos routers.

```
Gateway#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B
- BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-
IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is 209.165.201.17 to network 0.0.0.0

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/1
L        192.168.1.1/32 is directly connected, GigabitEthernet0/1
      209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.201.16/30 is directly connected, Serial0/0/1
L        209.165.201.18/32 is directly connected, Serial0/0/1
S* 0.0.0.0/0 [1/0] via 209.165.201.17
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
ISP(config)#do show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

192.31.7.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.31.7.0/24 is directly connected, GigabitEthernet0/0
L       192.31.7.1/32 is directly connected, GigabitEthernet0/0
209.165.200.0/27 is subnetted, 1 subnets
S       209.165.200.224/27 [1/0] via 209.165.201.18
209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.16/30 is directly connected, Serial0/0/0
L       209.165.201.17/32 is directly connected, Serial0/0/0
```

Parte 14. configurar y verificar la NAT estática.

La NAT estática consiste en una asignación uno a uno entre direcciones locales y globales, y estas asignaciones se mantienen constantes. La NAT estática resulta útil, en especial para los servidores web o los dispositivos que deben tener direcciones estáticas que sean accesibles desde Internet.

Paso 1. configurar una asignación estática.

El mapa estático se configura para indicarle al router que traduzca entre la dirección privada del servidor interno 192.168.1.20 y la dirección pública 209.165.200.225. Esto permite que los usuarios tengan acceso a la PC-A desde Internet. La PC-A simula un servidor o un dispositivo con una dirección constante a la que se puede acceder desde Internet.

```
Gateway(config)# ip nat inside source static 192.168.1.20 209.165.200.225
```

Paso 2. Especifique las interfaces.

Emita los comandos `ip nat inside` e `ip nat outside` en las interfaces.

```
Gateway(config)# interface g0/1
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
Gateway(config-if)# ip nat inside
Gateway(config-if)# interface s0/0/1
Gateway(config-if)# ip nat outside
```

Paso 3. probar la configuración.

- a. Muestre la tabla de NAT estática mediante la emisión del comando **show ip nat translations**.

```
Gateway# show ip nat translations
Pro Inside global    Inside local    Outside local    Outside global
--- 209.165.200.225  192.168.1.20    ---             ---

Gateway#show ip nat translations
Pro  Inside global    Inside local    Outside local
Outside global
---  209.165.200.225  192.168.1.20    ---             ---
```

¿Cuál es la traducción de la dirección host local interna?

192.168.1.20 = __209.165.200.225__

¿Quién asigna la dirección global interna?

__El router - el proveedor de internet__

¿Quién asigna la dirección local interna?

__Los administradores de red __

- b. En la PC-A, haga ping a la interfaz Lo0 (192.31.7.1) en el ISP. Si el ping falló, resuelva y corrija los problemas. En el router Gateway, muestre la tabla de NAT.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
SERVER>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=31ms TTL=254
Reply from 192.31.7.1: bytes=32 time=20ms TTL=254
Reply from 192.31.7.1: bytes=32 time=31ms TTL=254
Reply from 192.31.7.1: bytes=32 time=21ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 31ms, Average = 25ms

SERVER>ping 192.31.7.2

Pinging 192.31.7.2 with 32 bytes of data:

Reply from 192.31.7.2: bytes=32 time=38ms TTL=126
Reply from 192.31.7.2: bytes=32 time=16ms TTL=126
Reply from 192.31.7.2: bytes=32 time=39ms TTL=126
Reply from 192.31.7.2: bytes=32 time=36ms TTL=126

Ping statistics for 192.31.7.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 39ms, Average = 32ms
```

Gateway# **show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.200.225:1	192.168.1.20:1	192.31.7.1:1	192.31.7.1:1
---	209.165.200.225	192.168.1.20	---	---

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```

Gateway#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside
global
icmp 209.165.200.225:37 192.168.1.20:37   192.31.7.2:37     192.31.7.2:37
icmp 209.165.200.225:38 192.168.1.20:38   192.31.7.2:38     192.31.7.2:38
icmp 209.165.200.225:39 192.168.1.20:39   192.31.7.2:39     192.31.7.2:39
icmp 209.165.200.225:40 192.168.1.20:40   192.31.7.2:40     192.31.7.2:40
icmp 209.165.200.225:41 192.168.1.20:41   192.31.7.1:41     192.31.7.1:41
icmp 209.165.200.225:42 192.168.1.20:42   192.31.7.1:42     192.31.7.1:42
icmp 209.165.200.225:43 192.168.1.20:43   192.31.7.1:43     192.31.7.1:43
icmp 209.165.200.225:44 192.168.1.20:44   192.31.7.1:44     192.31.7.1:44
icmp 209.165.200.225:45 192.168.1.20:45   192.31.7.2:45     192.31.7.2:45
icmp 209.165.200.225:46 192.168.1.20:46   192.31.7.2:46     192.31.7.2:46
icmp 209.165.200.225:47 192.168.1.20:47   192.31.7.2:47     192.31.7.2:47
icmp 209.165.200.225:48 192.168.1.20:48   192.31.7.2:48     192.31.7.2:48
--- 209.165.200.225     192.168.1.20     ---               ---

```

Cuando la PC-A envió una solicitud de ICMP (ping) a la dirección 192.31.7.1 en el ISP, se agregó a la tabla una entrada de NAT en la que se indicó ICMP como protocolo.

¿Qué número de puerto se usó en este intercambio ICMP? __41__

Nota: puede ser necesario desactivar el firewall de la PC-A para que el ping se realice correctamente.

- c. En la PC-A, acceda a la interfaz Lo0 del ISP mediante telnet y muestre la tabla de NAT.

```

Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.225:1  192.168.1.20:1   192.31.7.1:1      192.31.7.1:1
tcp 209.165.200.225:1034 192.168.1.20:1034 192.31.7.1:23     192.31.7.1:23
--- 209.165.200.225     192.168.1.20     ---               ---

Gateway#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside
global
--- 209.165.200.225     192.168.1.20     ---               ---
tcp 209.165.200.225:1025 192.168.1.20:1025 192.31.7.2:80     192.31.7.2:80

```

Nota: es posible que se haya agotado el tiempo para la NAT de la solicitud de ICMP y se haya eliminado de la tabla de NAT.

¿Qué protocolo se usó para esta traducción? __Web__

¿Cuáles son los números de puerto que se usaron?

Global/local interno: __1025__

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Global/local externo: __80__

- d. Debido a que se configuró NAT estática para la PC-A, verifique que el ping del ISP a la dirección pública de NAT estática de la PC-A (209.165.200.225) se realice correctamente.

```
Packet Tracer SERVER Command Line 1.0
SERVER>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=3ms TTL=126
Reply from 209.165.200.225: bytes=32 time=16ms TTL=126
Reply from 209.165.200.225: bytes=32 time=13ms TTL=126
Reply from 209.165.200.225: bytes=32 time=12ms TTL=126

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 16ms, Average = 11ms
```

PC-A

Services

Desktop

Software/Services

HTTP

HTTP

☒ On ☐ Off

HTTPS

☒ On ☐ Off

File Name:

```

<html>
<h1>PCA</h1>
<center><font size='+2' color='blue'>Cisco Packet
Tracer</font></center>
<hr>Welcome to Cisco Packet Tracer. Opening doors to new
opportunities. Mind Wide Open.
<p>Quick Links:
<br><a href='helloworld.html'>A small page</a>
<br><a href='copyrights.html'>Copyrights</a>
<br><a href='image.html'>Image page</a>
<br><a href='cscoptlogo177x111.jpg'>Image</a>
</html>

```


UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



- e. En el router Gateway, muestre la tabla de NAT para verificar la traducción.

Gateway# **show ip nat translations**

```
Pro Inside global    Inside local    Outside local    Outside global
icmp 209.165.200.225:12 192.168.1.20:12 209.165.201.17:12
209.165.201.17:12
--- 209.165.200.225    192.168.1.20    ---            ---

Gateway#show ip nat translations
Pro  Inside global    Inside local    Outside local    Outside global
---  209.165.200.225    192.168.1.20    ---            ---
tcp  209.165.200.225:1025 192.168.1.20:1025 192.31.7.2:80    192.31.7.2:80
tcp  209.165.200.225:80 192.168.1.20:80 192.31.7.2:1025 192.31.7.2:1025
tcp  209.165.200.225:80 192.168.1.20:80 192.31.7.2:1026 192.31.7.2:1026
```

Observe que la dirección local externa y la dirección global externa son iguales. Esta dirección es la dirección de origen de red remota del ISP. Para que el ping del ISP se realice correctamente, la dirección global interna de NAT estática 209.165.200.225 se tradujo a la dirección local interna de la PC-A (192.168.1.20).

- f. Verifique las estadísticas de NAT mediante el comando **show ip nat statistics** en el router Gateway.

Gateway# **show ip nat statistics**

```
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Peak translations: 2, occurred 00:02:12 ago
Outside interfaces:
Serial0/0/1
```


UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Inside interfaces:

GigabitEthernet0/1

Hits: 39 Misses: 0

CEF Translated packets: 39, CEF Punted packets: 0

Expired translations: 3

Dynamic mappings:

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

```
Gateway#show ip nat statistics
Total translations: 4 (1 static, 3 dynamic, 3 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 56 Misses: 51
Expired translations: 48
Dynamic mappings:
```

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

Parte 15. configurar y verificar la NAT dinámica

La NAT dinámica utiliza un conjunto de direcciones públicas y las asigna según el orden de llegada. Cuando un dispositivo interno solicita acceso a una red externa, la NAT dinámica asigna una dirección IPv4 pública disponible del conjunto. La NAT dinámica produce una asignación de varias direcciones a varias direcciones entre direcciones locales y globales.

Paso 1. borrar las NAT.

Antes de seguir agregando NAT dinámicas, borre las NAT y las estadísticas de la parte 2.

```
Gateway# clear ip nat translation *
```

```
Gateway# clear ip nat statistics
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
Gateway#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
---  209.165.200.225     192.168.1.20     ---               ---
```

Paso 2. definir una lista de control de acceso (ACL) que coincida con el rango de direcciones IP privadas de LAN.

La ACL 1 se utiliza para permitir que se traduzca la red 192.168.1.0/24.

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

Paso 3. verificar que la configuración de interfaces NAT siga siendo válida.

Emita el comando `show ip nat statistics` en el router Gateway para verificar la configuración NAT.

```
Gateway#show ip nat statistics
Total translations: 1 (1 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 56 Misses: 51
Expired translations: 48
Dynamic mappings:
```

Paso 4. definir el conjunto de direcciones IP públicas utilizables.

```
Gateway(config)# ip nat pool public_access 209.165.200.242 209.165.200.254
netmask 255.255.255.224
```

Paso 5. definir la NAT desde la lista de origen interna hasta el conjunto externo.

Nota: recuerde que los nombres de conjuntos de NAT distinguen mayúsculas de minúsculas, y el nombre del conjunto que se introduzca aquí debe coincidir con el que se usó en el paso anterior.

```
Gateway(config)# ip nat inside source list 1 pool public_access
```

Paso 6. probar la configuración.

- En la PC-B, haga ping a la interfaz Lo0 (192.31.7.1) en el ISP. Si el ping falló, resuelva y corrija los problemas. En el router Gateway, muestre la tabla de NAT.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
PC>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=21ms TTL=254
Reply from 192.31.7.1: bytes=32 time=32ms TTL=254
Reply from 192.31.7.1: bytes=32 time=11ms TTL=254
Reply from 192.31.7.1: bytes=32 time=32ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 32ms, Average = 24ms
```

Gateway# **show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
---	209.165.200.225	192.168.1.20	---	---
icmp	209.165.200.242:1	192.168.1.21:1	192.31.7.1:1	192.31.7.1:1
---	209.165.200.242	192.168.1.21	---	---

```
Gateway#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.242:33 192.168.1.21:33  192.31.7.1:33     192.31.7.1:33
icmp 209.165.200.242:34 192.168.1.21:34  192.31.7.1:34     192.31.7.1:34
icmp 209.165.200.242:35 192.168.1.21:35  192.31.7.1:35     192.31.7.1:35
icmp 209.165.200.242:36 192.168.1.21:36  192.31.7.1:36     192.31.7.1:36
---  209.165.200.225    192.168.1.20     ---                ---
```

¿Cuál es la traducción de la dirección host local interna de la PC-B?

192.168.1.21 = 209.165.200.242

Cuando la PC-B envió un mensaje ICMP a la dirección 192.31.7.1 en el ISP, se agregó a la tabla una entrada de NAT dinámica en la que se indicó ICMP como el protocolo.

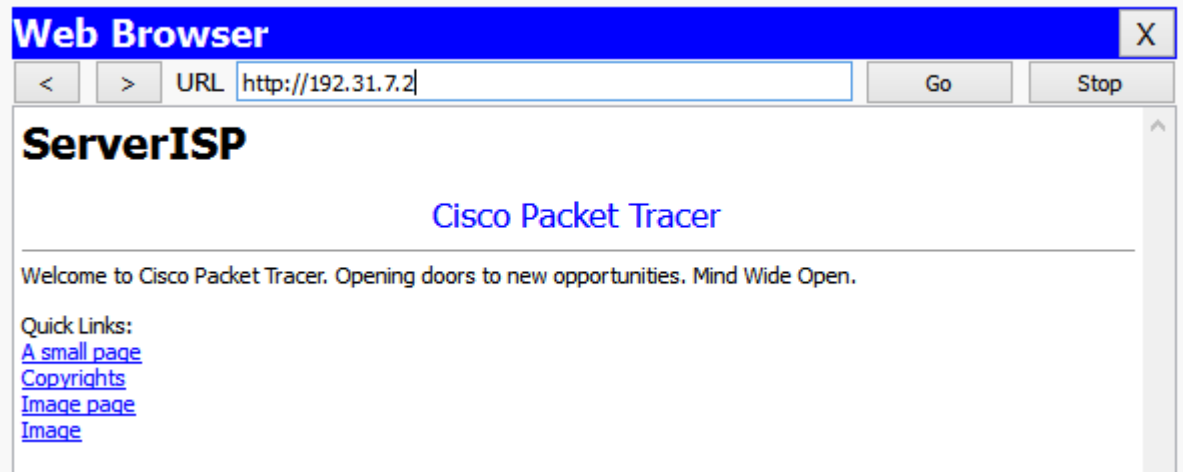
¿Qué número de puerto se usó en este intercambio ICMP? 33

- En la PC-B, abra un explorador e introduzca la dirección IP del servidor web simulado ISP (interfaz Lo0). Cuando se le solicite, inicie sesión como **webuser** con la contraseña **webpass**.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Para nuestro caso ingresamos por el web browser:



c. Muestre la tabla de NAT.

Pro	Inside global	Inside local	Outside local	Outside global
---	209.165.200.225	192.168.1.20	---	---
tcp	209.165.200.242:1038	192.168.1.21:1038	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1039	192.168.1.21:1039	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1040	192.168.1.21:1040	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1041	192.168.1.21:1041	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1042	192.168.1.21:1042	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1043	192.168.1.21:1043	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1044	192.168.1.21:1044	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1045	192.168.1.21:1045	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1046	192.168.1.21:1046	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1047	192.168.1.21:1047	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1048	192.168.1.21:1048	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1049	192.168.1.21:1049	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1050	192.168.1.21:1050	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1051	192.168.1.21:1051	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1052	192.168.1.21:1052	192.31.7.1:80	192.31.7.1:80
---	209.165.200.242	192.168.1.22	---	---

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
Gateway#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
---  209.165.200.225     192.168.1.20      ---               ---
tcp  209.165.200.242:1025 192.168.1.21:1025 192.31.7.2:80     192.31.7.2:80
```

¿Qué protocolo se usó en esta traducción? _Http__

¿Qué números de puerto se usaron?

Interno: __1025__

Externo: __80__

¿Qué número de puerto bien conocido y qué servicio se usaron? __el http usó el 80__

- d. Verifique las estadísticas de NAT mediante el comando **show ip nat statistics** en el router Gateway.

Gateway# **show ip nat statistics**

Total active translations: 3 (1 static, 2 dynamic; 1 extended)

Peak translations: 17, occurred 00:06:40 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 345 Misses: 0

CEF Translated packets: 345, CEF Punted packets: 0

Expired translations: 20

Dynamic mappings:

-- Inside Source

[Id: 1] access-list 1 pool public_access refcount 2

pool public_access: netmask 255.255.255.224

start 209.165.200.242 end 209.165.200.254

type generic, total addresses 13, allocated 1 (7%), misses 0

Total doors: 0

Appl doors: 0

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Normal doors: 0
Queued Packets: 0

```
Gateway#show ip nat statistics
Total translations: 2 (1 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 71 Misses: 84
Expired translations: 56
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 1
 pool public_access: netmask 255.255.255.224
   start 209.165.200.242 end 209.165.200.254
   type generic, total addresses 13 , allocated 1 (7%), misses 0
```

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

Paso 7. eliminar la entrada de NAT estática.

En el paso 7, se elimina la entrada de NAT estática y se puede observar la entrada de NAT.

- Elimine la NAT estática de la parte 2. Introduzca **yes** (sí) cuando se le solicite eliminar entradas secundarias.

Gateway(config)# **no ip nat inside source static 192.168.1.20 209.165.200.225**

Static entry in use, do you want to delete child entries? [no]: **yes**

- Borre las NAT y las estadísticas.
- Haga ping al ISP (192.31.7.1) desde ambos hosts.
- Muestre la tabla y las estadísticas de NAT.

Gateway# **show ip nat statistics**

Total active translations: 4 (0 static, 4 dynamic; 2 extended)

Peak translations: 15, occurred 00:00:43 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
GigabitEthernet0/1
Hits: 16 Misses: 0
CEF Translated packets: 285, CEF Punted packets: 0
Expired translations: 11
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 4
  pool public_access: netmask 255.255.255.224
    start 209.165.200.242 end 209.165.200.254
    type generic, total addresses 13, allocated 2 (15%), misses 0
```

```
Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Gateway# **show ip nat translation**

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.200.243:512	192.168.1.20:512	192.31.7.1:512	192.31.7.1:512
---	209.165.200.243	192.168.1.20	---	---
icmp	209.165.200.242:512	192.168.1.21:512	192.31.7.1:512	192.31.7.1:512
---	209.165.200.242	192.168.1.21	---	---

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
Gateway#show ip nat statistics
Total translations: 1 (0 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 71 Misses: 84
Expired translations: 56
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 1
 pool public_access: netmask 255.255.255.224
   start 209.165.200.242 end 209.165.200.254
   type generic, total addresses 13 , allocated 1 (7%), misses 0
Gateway#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
tcp 209.165.200.242:1025 192.168.1.21:1025 192.31.7.2:80      192.31.7.2:80
```

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

Reflexión

1. ¿Por qué debe utilizarse la NAT en una red?

Debido a que las ipv4 se estaban acabando se implementó utilizar para un grupo de red privadas el uso de una sola red pública, de esta manera se realiza un ahorro de Ip porque varias pc pueden ingresar a internet con la misma Ip pública (Aumenta la flexibilidad de las conexiones con la red pública). Adicional a esto aumenta el nivel de seguridad, un usuario no aparece en internet con su Ip privada, sino con la Ip pública asignada.

2. ¿Cuáles son las limitaciones de NAT?

Entre su desventajas esta que algunas aplicaciones que utilizan el direccionamiento IP dejan de funcionar, porque esconde las direcciones IP de extremo a extremo, no todas las aplicaciones y protocolos son compatibles con NAT; también aumenta el retardo y necesita mayor potencia de computación.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet n.º 2	Interfaz serial #1	Interfaz serial n.º 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
<p>Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.</p>				

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Laboratorio 11.2.3.7 Configuración de un conjunto de nat con sobrecarga y pat

Topología

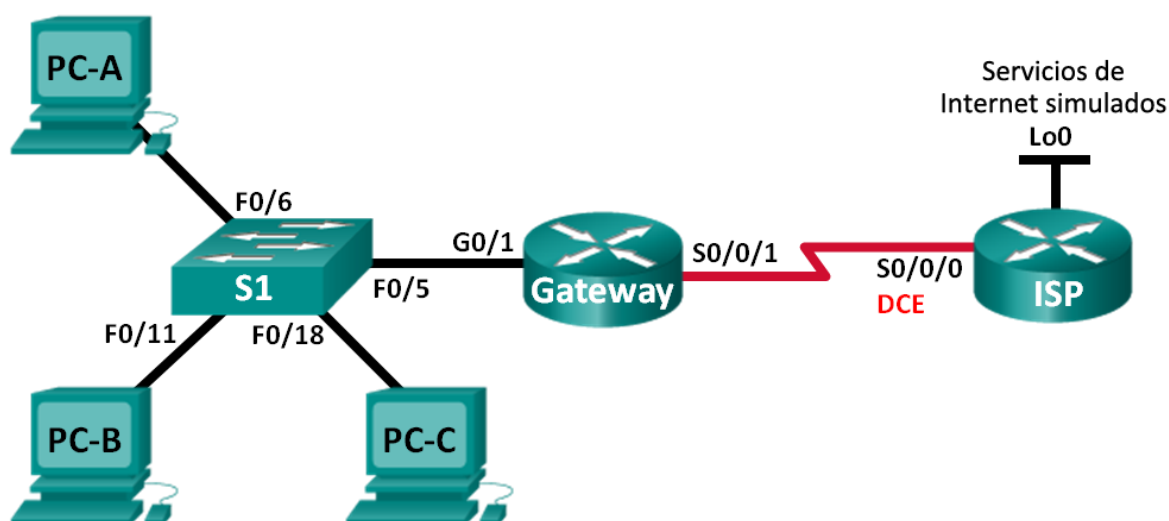


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
PC-A	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.22	255.255.255.0	192.168.1.1

Objetivos

Parte 1: armar la red y verificar la conectividad

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Parte 2: configurar y verificar un conjunto de NAT con sobrecarga

Parte 3: configurar y verificar PAT

Recursos necesarios

2 ROUTERS (CISCO 1941 CON IOS DE CISCO VERSIÓN 15.2(4)M3, IMAGEN UNIVERSAL O SIMILAR)

1 SWITCH (CISCO 2960 CON IOS DE CISCO VERSIÓN 15.0(2), IMAGEN LANBASEK9 O COMPARABLE)

3 COMPUTADORAS (WINDOWS 7, VISTA O XP CON UN PROGRAMA DE EMULACIÓN DE TERMINAL, COMO TERA TERM)

CABLES DE CONSOLA PARA CONFIGURAR LOS DISPOSITIVOS CON IOS DE CISCO MEDIANTE LOS PUERTOS DE CONSOLA

CABLES ETHERNET Y SERIALES, COMO SE MUESTRA EN LA TOPOLOGÍA

Parte 1. armar la red y verificar la conectividad

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de interfaz, el routing estático, el acceso a los dispositivos y las contraseñas.

Paso 8. realizar el cableado de red tal como se muestra en la topología.

Paso 9. configurar los equipos host.

Paso 10. inicializar y volver a cargar los routers y los switches.

Paso 11. configurar los parámetros básicos para cada router.

- a. Desactive la búsqueda del DNS.
- b. Configure las direcciones IP para los routers como se indica en la tabla de direccionamiento.
- c. Establezca la frecuencia de reloj en **128000** para la interfaz serial DCE.
- d. Configure el nombre del dispositivo como se muestra en la topología.
- e. Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- f. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



- g. Configure **logging synchronous** para evitar que los mensajes de consola interrumpen la entrada del comando.

Paso 12. configurar el routing estático.

- a. Cree una ruta estática desde el router ISP hasta el router Gateway.
ISP(config)# **ip route 209.165.200.224 255.255.255.248 209.165.201.18**
- b. Cree una ruta predeterminada del router Gateway al router ISP.
Gateway(config)# **ip route 0.0.0.0 0.0.0.0 209.165.201.17**

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 209.165.200.224 255.255.255.248 209.165.201.18
Router(config)#hostname ISP
ISP(config)#ip route 209.165.200.224 255.255.255.248 209.165.201.18
ISP(config)#
```

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Gateway
Gateway(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.17
Gateway(config)#
```

Paso 13. Verificar la conectividad de la red

- a. Desde los equipos host, haga ping a la interfaz G0/1 en el router Gateway. Resuelva los problemas si los pings fallan.
- b. Verifique que las rutas estáticas estén bien configuradas en ambos routers.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=32ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 32ms, Average = 8ms

PC>
```

Parte 16. configurar y verificar el conjunto de NAT con sobrecarga

En la parte 2, configurará el router Gateway para que traduzca las direcciones IP de la red 192.168.1.0/24 a una de las seis direcciones utilizables del rango 209.165.200.224/29.

Paso 1. definir una lista de control de acceso que coincida con las direcciones IP privadas de LAN.

La ACL 1 se utiliza para permitir que se traduzca la red 192.168.1.0/24.

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

Paso 2. definir el conjunto de direcciones IP públicas utilizables.

```
Gateway(config)# ip nat pool public_access 209.165.200.225 209.165.200.230
netmask 255.255.255.248
```

Paso 3. definir la NAT desde la lista de origen interna hasta el conjunto externo.

```
Gateway(config)# ip nat inside source list 1 pool public_access overload
```

Paso 4. Especifique las interfaces.

Emita los comandos ip nat inside e ip nat outside en las interfaces.

```
Gateway(config)# interface g0/1
Gateway(config-if)# ip nat inside
Gateway(config-if)# interface s0/0/1
```

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Gateway(config-if)# ip nat outside

```
Gateway(config)#  
Gateway(config)#access-list 1 permit 192.168.1.0 0.0.0.255  
Gateway(config)#ip nat pool public_access 209.165.200.225  
209.165.200.230 netmask 255.255.255.248  
Gateway(config)#ip nat inside source list 1 pool public_access overload  
Gateway(config)#interface g0/1  
Gateway(config-if)#ip nat inside  
Gateway(config-if)#interface s0/0/1  
Gateway(config-if)#ip nat outside  
Gateway(config-if)#exit  
Gateway(config)#exit  
Gateway#  
%SYS-5-CONFIG_I: Configured from console by console  
Gateway#
```

Paso 5. verificar la configuración del conjunto de NAT con sobrecarga.

- Desde cada equipo host, haga ping a la dirección 192.31.7.1 del router ISP.
- Muestre las estadísticas de NAT en el router Gateway.

Gateway# **show ip nat statistics**

Total active translations: 3 (0 static, 3 dynamic; 3 extended)

Peak translations: 3, occurred 00:00:25 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 24 Misses: 0

CEF Translated packets: 24, CEF Punted packets: 0

Expired translations: 0

Dynamic mappings:

-- Inside Source

[Id: 1] access-list 1 pool public_access refcount 3

pool public_access: netmask 255.255.255.248

start 209.165.200.225 end 209.165.200.230

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



type generic, total addresses 6, allocated 1 (16%), misses 0

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

c. Muestre las NAT en el router Gateway.

Gateway# **show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.200.225:0	192.168.1.20:1	192.31.7.1:1	192.31.7.1:0
icmp	209.165.200.225:1	192.168.1.21:1	192.31.7.1:1	192.31.7.1:1
icmp	209.165.200.225:2	192.168.1.22:1	192.31.7.1:1	192.31.7.1:2

Nota: es posible que no vea las tres traducciones, según el tiempo que haya transcurrido desde que hizo los pings en cada computadora. Las traducciones de ICMP tienen un valor de tiempo de espera corto.

¿Cuántas direcciones IP locales internas se indican en el resultado de muestra anterior? 3

¿Cuántas direcciones IP globales internas se indican? 1

¿Cuántos números de puerto se usan en conjunto con las direcciones globales internas? 12

¿Cuál sería el resultado de hacer ping del router ISP a la dirección local interna de la PC-A? ¿Por qué?

El Ping fallaría ya que su dirección no se muestra para la salida sino se muestra una IP para salir hacia Internet. Porque NAT las protege y no deja que ISP las conozca por su IP original si no las que les pone NAT
configurar y verificar PAT

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



En la parte 3, configurará PAT mediante el uso de una interfaz, en lugar de un conjunto de direcciones, a fin de definir la dirección externa. No todos los comandos de la parte 2 se volverán a usar en la parte 3.

Paso 6. borrar las NAT y las estadísticas en el router Gateway.

Paso 7. verificar la configuración para NAT.

- Verifique que se hayan borrado las estadísticas.
- Verifique que las interfaces externa e interna estén configuradas para NAT.
- Verifique que la ACL aún esté configurada para NAT.

¿Qué comando usó para confirmar los resultados de los pasos a al c?

Show ip nat etatistics

Paso 8. eliminar el conjunto de direcciones IP públicas utilizables.

```
Gateway(config)# no ip nat pool public_access 209.165.200.225  
209.165.200.230 netmask 255.255.255.248
```

Paso 9. eliminar la traducción NAT de la lista de origen interna al conjunto externo.

```
Gateway(config)# no ip nat inside source list 1 pool public_access overload
```

Paso 10. asociar la lista de origen a la interfaz externa.

```
Gateway(config)# ip nat inside source list 1 interface serial 0/0/1 overload
```

Paso 11. probar la configuración PAT.

- Desde cada computadora, haga ping a la dirección 192.31.7.1 del router ISP.
- Muestre las estadísticas de NAT en el router Gateway.

```
Gateway# show ip nat statistics
```

```
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
```

```
Peak translations: 3, occurred 00:00:19 ago
```

```
Outside interfaces:
```

```
Serial0/0/1
```

```
Inside interfaces:
```


UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



GigabitEthernet0/1
Hits: 24 Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source

[Id: 2] access-list 1 interface Serial0/0/1 refcount 3

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0

c. Muestre las traducciones NAT en el Gateway.

Gateway# **show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.201.18:3	192.168.1.20:1	192.31.7.1:1	192.31.7.1:3
icmp	209.165.201.18:1	192.168.1.21:1	192.31.7.1:1	192.31.7.1:1
icmp	209.165.201.18:4	192.168.1.22:1	192.31.7.1:1	192.31.7.1:4

Reflexión

¿Qué ventajas tiene la PAT?

- Al utilizarse solo una IP pública que es la del interface se ahorran direcciones IP públicas, pueden salir 100 computadoras de una red privada con direcciones privadas con una sola IP pública y utilizando distintos puertos para diferenciar cada paquete que sale.
- Nivel de seguridad

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet n.º 2	Interfaz serial #1	Interfaz serial n.º 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
<p>Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.</p>				

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I

CONCLUSIONES

- Por medio del anterior trabajo, pudimos dar práctica a la unidad 4 del diplomado de profundización de cisco, logrando identificar, enrutamiento en soluciones de red.
- La práctica hace al maestro, por esto, gracias a los ejercicios prácticos podemos adquirir las cualidades de un buen administrador de redes.
- Enfrentándose a una problemática en una red, el estudiante afianza los conocimientos adquiridos estando en capacidad de resolver de la mejor manera la necesidad de un caso en particular.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
DIPLOMADO DE PROFUNDIZACION CISCO
2017 I



REFERENCIAS

- Amberg, E. (2014). CCNA 1 Powertraining : ICND1/CCENT (100-101). Heidelberg: MITP. Recuperado de: <http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=e000xww&AN=979032&lang=es&site=ehost-live>
- Lammle, T. (2008). Todd Lammle's CCNA IOS Commands Survival Guide. Indianapolis, Ind: Sybex. Recuperado de: <http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=e000xww&AN=218603&lang=es&site=ehost-live>
- Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de: <http://een.iust.ac.ir/profs/Beheshti/Computer%20networking/Auxiliary%20materials/Cisco-ICND2.pdf>
- Lammle, T. (2010). CISCO Press (Ed). Cisco Certified Network Associate Study Guide. Recuperado de: <http://gonda.nic.in/swangonda/pdf/ccna1.pdf>
- UNAD (2014). Principios de Enrutamiento [OVA]. Recuperado de: https://1drv.ms/u/s!AmlJYei-NT1lhgOyjWeh6timi_Tm
- CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1>
- CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>
- CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1>
- CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>
- CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1>